UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL

DIRECCIÓN GENERAL DE POSGRADOS

MAESTRÍA EN TELEINFORMÁTICA Y REDES DE COMPUTADORES

Trabajo de Grado para la obtención

Del título de:

Magíster en Teleinformática y Redes de Computadores

TÌTULO

DISEÑO E IMPLEMENTACIÓN DE IPv6 (PROTOCOLO DE DIRECCIONAMIENTO IP VERSIÓN 6) E *IPsec* (PROTOCOLO DE INTERNET SEGURO) EN LAS INTRANETS Y EXTRANET QUE CONFORMAN LA RED DE DATOS DE LA UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL.

Autor

Ing. Freddy Armando Velasteguí Barragán

Director

Ing. Juan Carlos Rivera Gaibor, MBA

Quito, Ecuador

Junio – 2012

HOJA DE RESPONSABILIDAD

EL PRESENTE TRABAJO DE GRADO CONSTITUYE UN REQUISITO PREVIO PARA LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN TELEINFORMÁTICA Y REDES DE COMPUTADORES.

Yo, **FREDDY ARMANDO VELASTEGUÍ BARRAGÁN**, declaro que la realización de este trabajo, los resultados y conclusiones obtenidas son de absoluta responsabilidad del autor. La mala utilización del mismo o fines no vinculados a la Universidad Tecnológica Equinoccial no son responsabilidad de la autoría.

_____

CI: 1708971005

INFORME DEL DIRECTOR

Quito, 16 de Noviembre de 2011

Ingeniero

Carlos Trueba Piedrahita

Director General de Posgrados

De mi consideración.

Por medio de la presente me dirijo a usted para indicarle que, yo: Juan Carlos Rivera designando como Director del Trabajo de Grado, Titulado: “Diseño e Implementación de IPv6 (protocolo de direccionamiento IP versión 6) e *IPsec* (protocolo de internet seguro) en las intranets y extranet que conforman la red de datos de la Universidad Tecnológica Equinoccial” realizado por el maestrante: Freddy Armando Velasteguí Barragán, ha sido concluido.

Además certifico que el presente Trabajo de Tesis cumple todas las condiciones y requerimientos planteadas por el Instituto de Posgrado de la Universidad Tecnológica Equinoccial.

El estudiante ha cumplido con todos los procedimientos de revisión, estandarización y corrección establecidos para realizar este proyecto bajo mi tutoría del cual fui designado como Director.

Por la atención prestada anticipo mi agradecimiento.

Atentamente,

Juan Carlos Rivera
Director de Tesis

AGRADECIMIENTO

A Dios que fortaleció mi espíritu con mucha fe y me ha dado la existencia en este mundo para vivir y sentir la meta de culminar este proyecto.

A los seres que más amo; mi esposa y mi hijo, lo mejor de mi vida que basta con su presencia para tener el deseo de luchar día a día y quienes me han transmitido la energía necesaria para seguir adelante. ¡Juntos lo hemos logrado!

A mis padres que con su ejemplo y perseverancia siempre han estado a mi lado, mis hermanas, sobrinos y cuñado que han estado pendientes de mí. Muchas gracias.

A mis queridos suegros y cuñada que con su humildad y cariño me han apoyado tanto.

Al Ingeniero Juan Carlos Rivera; que con su guía y ejemplo intachable me ha llevado a lograr este proyecto.

A mis primos, tíos y toda mi familia que me han dado siempre su mano en los momentos que más he necesitado.

Gracias a todos de todo corazón.

Freddy A. Velasteguí B.

DEDICATORIA

Este trabajo de grado lo dedico a Dios, que me ha enseñado a valorar la vida espiritual con amor, paciencia y Fe.

Por quienes sigo existiendo; mi esposa Stefita, que en los momentos más difíciles de mi vida en los que vi la obscuridad, me encendió la luz con su verdadero amor y extremada paciencia para poder continuar. Mi hijo Michaelito Armado que con su forma de ser, inocencia y ternura me llena de tanto amor, por ustedes quiero ser el mejor. ¡Los amo!

Padre y Madre gracias por traerme al mundo y por permitirme siempre contar con ustedes, su ejemplo es mi remedio.

Mis queridas Ñañas; Yeya y Pam por siempre juntos. Luka y Martín; mis adorados sobrinos la alegría de la familia.

Mis queridos suegros; Mery y Ramiro con sus pensamientos, bondad y trabajo han sido el pilar para que hagan realidad algunos de mis sueños.

Mi linda Cuñada Michelle una persona especial en mi vida que vi crecer desde que era una niña, muchas gracias por estar junto a mí.

Tío George y Rosita; con su don de gente me abrieron el corazón y ahí estamos.

Fab y Sebitas con la AKD hasta el fin del mundo.

A mis compañeros de trabajo por su gran solidaridad.

A todas las personas que cuando estaba en el Hospital me empujaron siempre para adelante.

"El Cáncer es el síntoma de un amor mal entendido. El Cáncer solo respeta el símbolo del amor verdadero. El símbolo del amor verdadero es el corazón. El corazón es el único órgano que no es atacado por el Cáncer."

(Anónimo)

TABLA DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

INDICE DE TABLAS

RESUMEN

El presente proyecto de grado está estructurado de la siguiente manera:

En el Capítulo I, se menciona en una forma más amplia el objetivo general, objetivos específicos, alcance, justificación, marco de referencia y la estrategia metodológica, aprobados en el plan de tesis.

En el Capítulo II, se realiza un estudio y descripción del protocolo de direccionamiento IPv6 desde el punto de vista teórico, especificando la estructura y las características que dispone este protocolo; además se realiza una descripción de las ventajas, diferencias y nuevas funcionalidades con el actual protocolo IPv4 ya implementado.

En el Capítulo III, se realiza un análisis de la situación actual de la red de la Universidad Tecnológica Equinoccial con su sistema de direccionamiento IPv4 y un inventario del hardware y software para su compatibilidad con IPv6. Para ello, el estudio se ha segmentado en tres aspectos importantes: LAN, WAN y acceso a Internet.

En el Capítulo IV, se realiza el diseño y la implementación del nuevo protocolo IPv6 en donde se detalla las configuraciones de los dispositivos que permiten y soportan IPv6 y se realiza los diagramas con el nuevo direccionamiento IPv6 basándose en el IPv4.

En el Capítulo V se indican las conclusiones finales del proyecto y las recomendaciones que deben considerarse al implementar IPv6.

ABSTRACT

This graduation present project has been structured into chapters. They are;

Chapter I, into this chapter, its general objective, the specific ones, its complete coverage, justification; referential frame and its methodological strategy are treated over here in a wider way.

Chapter II, The directional IPv6 protocol is analyzed and descripted from theoretical point of view by specifying its structure and characteristics that this protocol provides. Furthermore a description of the advantages, differences and new functions with the present IPv4 protocol already implemented is treated into this chapter.

Chapter III, An analysis of the present situation of UTE informatics net is performed over here with its IPv4 directional system and its hardware and software inventory for relating compatibly with IPv6 protocol. For this purpose, the study has been divided into three important aspects, which are: LAN, WAN and internet access.

Chapter IV, A design and implementation of the new IPv6 protocol is performed over here, where all the configurations and new devices let the IPv6 protocol perform, diagrams with a new directional IPv6based on the IPv4 protocol.

Chapter V. Final conclusions and recommendations for implementing the IPv6 protocol are considered along this study.

CAPÍTULO I

INTRODUCCIÓN

La Universidad Tecnológica Equinoccial ha evolucionado tan rápidamente como la tecnología informática en el mundo entero; en la que el intercambio de datos, voz, video, imágenes y audio se unifican en la red, cuyos servicios generados demandan gran disponibilidad, fiabilidad, escalabilidad, seguridad y alta velocidad de transmisión.

En la actualidad la Universidad cuenta con equipo *networking* de última tecnología, que interconectan los diferentes edificios y bloques, y que constituyen la columna vertebral (*backbone*) de fibra óptica de alta velocidad; cuenta también con un cableado estructurado estandarizado, normalizado y certificado.

Sin embargo, mantiene un esquema de direccionamiento IPv4 que presenta algunas limitaciones al funcionamiento y demanda de las redes actuales y futuras, además IPv4 no fue diseñado para ser seguro.

El protocolo IPv6, es una nueva tecnología que está en auge, y que poco a poco está reemplazando al actual protocolo IPv4, que ha presentado problemas de seguridad y disponibilidad de números de direcciones.IPv6 es una evolución de IPv4 en la que se mejora la eficiencia y seguridad, conocida comúnmente como IPNG (*Internet Protocol Next Generation*). La versión de este protocolo es el 6 frente a la versión 4 utilizada hasta ahora, la versión 5 no pasó de la fase experimental.

Los cambios que se introducen en esta nueva versión son muchos y de gran importancia.

La transición desde la versión 4 presentan características de compatibilidad que se han incluido en el IPv6, el cual se ha diseñado para solucionar todos los problemas que surgen con la versión anterior, y además ofrecer soporte a las nuevas redes de alto rendimiento (como ATM para las WAN y *Gigabit-Ethernet* para las LAN).

Una de las características principales es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 bits, eliminando todas las restricciones del sistema actual. Además, el nuevo formato de la cabecera se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal.

Sin duda que IPv6 constituye una tecnología que se ha publicado con todos los estándares y mejoras que IPv4 ha experimentado con el transcurrir de los años, recordando que nació junto con el protocolo TCP /IP de una red con fines militares por agosto de 1977.

De acuerdo a las características de IPv4 se decía que las direcciones jamás se acabarían pero en la actualidad realmente no existen direcciones disponibles, lo que indica que migrar a IPv6 es la opción más acertada para un mejor manejo de las redes actuales.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Diseñar e implementar un esquema de direccionamiento IP seguro con IPv6 e *IPsec*, en la red de la Universidad Tecnológica Equinoccial.

1.2 OBJETIVOS ESPECÍFICOS

a) Determinar la situación actual de los sistemas operativos, aplicaciones y dispositivos que funcionan con IPv4 y migraran a IPv6.

b) Cuantificar los recursos que se involucraran sobre IPv6.

c) Diseñar una solución para implementar un esquema consolidado que trabaje con los sistemas para que se pueda conseguir resultados eficaces, confiables, rápidos, seguros y rentables.

d) Recomendar el software y hardware de última tecnología para aprovechar al máximo el protocolo IPv6.

e) Exponer e indicar las conclusiones y recomendaciones que implica implementar IPv6

1.3 JUSTIFICACIÓN

El direccionamiento IPv4 que maneja la UTE presenta limitaciones al funcionamiento de las redes actuales y futuras, tales como:

- Direcciones IP agotadas
- Ruteo ineficiente
- Obstaculiza el uso de Internet a nuevos usuarios
- Difícil adecuaciones a nuevas aplicaciones
- Uso necesario de NAT
- Arquitectura plana
- Direcciones de 32 Bits
- Configuración Manual
- *Broadcast*
- Sin identificación de *QoS*
- Seguridad Opcional

IPv6 supera todas estas limitaciones y ofrece:

- Direcciones de 132 bits
- Arquitectura Jerárquica
- Configuración Automática
- *Multicast* y *anycast*
- Seguridad obligatoria

Por esta razón se ha visto la necesidad de actualizar y automatizar sus sistemas, minimizando los problemas que les permitirán tener una alta disponibilidad, confiabilidad y eficiencia.

Para la actualización existe una gran variedad de soluciones que se presentarán aquí y de las propuestas que se cree que pueden definir el uso futuro de los recursos informáticos de la Universidad Tecnológica Equinoccial, propuestas que serán obtenidas a través de la investigación minuciosa de lo que actualmente sucede en la Universidad y que se espera sea un aporte al progreso socio-económico y cultural de la institución.

La Universidad Tecnológica Equinoccial como miembro de CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado), debe implementar IPv6 como un requerimiento de esta nueva Red de Internet 2.

Motivo por el cual el personal que administra los recursos informáticos de la Universidad Tecnológica Equinoccial requiere de una solución completa a este esquema presentado.

No es la tecnología la que cambiará a las personas o la que cambiará el curso de nuestras vidas, sino cómo se utilice y regule esos avances tecnológicos. Es importante tomar lo mejor de la tecnología y aplicarlo de una manera adecuada de acuerdo a las necesidades del ser humano.

1.4 ALCANCE

Para conseguir este proyecto, se expone los siguientes pasos secuenciales, que ayudarán a obtener resultados positivos en la consecución de los objetivos propuestos.

Realizar un análisis para evaluar que dispositivos y aplicaciones, que están implementados actualmente en la red de datos de la Universidad, soportarán e interactuarán con IPv6 e *IPsec*.

Proponer la mejor manera para migrar sistemas operativos, aplicaciones y programas hacia la nueva generación IP.

Implementar opciones para consolidar la intranet y el extranet sobre IPv6 conjuntamente con un protocolo seguro como lo es *IPsec*.

1.5 MARCO DE REFERENCIA

1.5.1 Marco teórico

Sería muy largo realizar un análisis de cómo se desarrolló en el mundo el proceso de comunicación. El hombre y los animales hasta hoy en día, pueden comunicarse por señas, sonidos, movimientos corporales, etc. Y luego la escritura, un avance fabuloso.

En épocas antiguas se recuerda como el hombre se comunicaba con sonidos (tambores), señales de humo, banderolas, haces de luz, etc.; para luego con el avance de la ciencia y conocimiento de la Física, una de cuyas divisiones es la electricidad y la mecánica, se puede construir el emisor y receptor del alfabeto Morse. Para llegar poco a poco a lo que es la comunicación alámbrica e inalámbrica como lo es el teléfono; y luego el mensaje escrito que hoy lo podemos visualizar y oírlo, como una de las conquistas más importantes del conocimientos

y de una de las materias científicas que más ha aportado al avance de la tecnología actual de la humanidad como lo es la Electrónica, conocimientos que han permitido mover el mundo entero con solo aplastar un botón o producir un mensaje de voz; increíble como con componentes casi macro se puede realizar tareas jamás soñadas y rapidez y facilidad fascinantes.

El desarrollo fabuloso de la Electrónica aplicado a los ordenadores, han facilitado todas o casi todas las tareas y los procesos en todos los campos Científicos y Tecnológicos del ser humano.

Hoy maravillados, aunque para muchos sin saber cuánto trabajo le costó a la Ciencia y Tecnología, poder comunicarse en fracciones de segundo, ofreciendo y/o receptando datos detallados y minuciosos, de todo lo que se necesita entre oficinas de una misma empresa, entre empresas, empresas y ciudades, entre países y entre continentes, sin que haya un solo conocimiento de cualquier índole que no pueda estar al alcance de nuestras manos.

La unificación de todos éstos culminó con la red de redes actualmente llamada Internet, que experimentó un crecimiento enorme que ha venido combinado con el hecho de que hay desperdicio de direcciones en muchos casos, provocando que ya hace varios años escaseen las direcciones IPv4.

Esta limitación impulso el aparecimiento de IPv6, que está actualmente en procesos de implementación, y se espera que termine reemplazando a IPv4.

IPv6 (*Internet Protocol Version* 6) o IPng (*Next Generation Internet Protocol*) es la nueva versión del protocolo IP (*Internet Protocol*). Ha sido diseñado por el IETF (*Internet Engineering TaskForce*) para reemplazar en forma gradual a la versión actual, el IPv4.

En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características.

El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

Otros de los problemas de IPv4 es la gran dimensión de las tablas de ruteo en el *backbone* de Internet, que lo hace ineficaz y perjudica los tiempos de respuesta.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la Calidad de Servicio (*QoS*), Seguridad (*IPsec*) y movilidad.

Formato de las direcciones global *unicast*.

Figura 1-1. Formato n-bits de las direcciones global *unicast*
Fuente: Red Académica Uruguaya, Proyecto IPv6, www.rau.edu.uy/IPv6/queesipv6.htm
Elaborado por: El Autor

Prefijo de ruteo global: es un prefijo asignado a un sitio, generalmente está estructurado jerárquicamente por los RIR e ISP.

Identificador de Subred: es el identificador de una subred dentro de un sitio. Está diseñado para que los administradores de los sitios lo estructuren jerárquicamente.

Identificador de Interfaz: es el identificador de una interfaz. En todas las direcciones *unicast*, excepto las que comienzan con el valor binario 000, el identificador de interfaz debe ser de 64 bits y estar construido en el formato *Modified* EUI-64.

El formato para este caso es el siguiente:

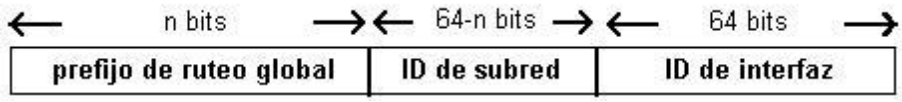

Figura 1-2. Formato64 bits de las direcciones global *unicast*
Fuente: Red Académica Uruguaya, Proyecto IPv6,www.rau.edu.uy/IPv6/queesipv6.htm
Elaborado por: El Autor

El siguiente es un ejemplo del formato de direcciones global *unicast* bajo el prefijo 2000::/3 administrado por el IANA (*Internet Assigned Numbers Authority*).

IPv6 es la evolución de IPv4, actual Protocolo de TCP/IP que permite la interconexión de millones de dispositivos sobre la red Internet, cada dispositivo de la red tiene direcciones IP distintas, lo que es utilizado por el protocolo para garantizar que los paquetes de información alcancen el destino correcto. IPv6 garantizará el futuro de Internet con la llegada de nuevos dispositivos y el soporte para seguridad. Cuenta con direcciones de longitud de 128 bits, frente a los 32 bits de IPv4, aumentando el número de direcciones IP disponibles desde 4 billones hasta 240 trillones de trillón.

Y esto último es lo que se propone implementar en la Universidad Tecnológica Equinoccial gracias a los avances y conocimientos Científicos y Tecnológicos que se han adquirido por parte del personal que administran los recursos informáticos de la Universidad.

1.5.2 Marco Conceptual

Desarrollo.- "Crecimiento intelectual del individuo adquirido por el ejercicio mental del aprendizaje de la enseñanza empírica"

Psicología de la educación, (2009). Consultado 31 de Enero del 202 (http://www.psicopedagogia.com/definicion)

Implementación.- "La implementación consiste en elaborar un diagnóstico sobre el grado de cumplimiento de los requisitos establecidos en una determinada norma de calidad e identificar las no conformidades y luego realizar las acciones

que permitan dar cumplimiento a todos los requisitos especificados". Implementación de Sistemas, (2008). Consultado el 31 de Enero de 2012 (http://www.camcapacitacion.cl/consultora.html)

Protocolo de red.- ‘‘Se conoce como protocolo de comunicaciones a un conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre sistemas". Diccionario de Informática, (1998 - 2011). Consultado 5 de Agosto 2011(http://www.alegsa.com.ar/Dic/)

IPv4.- "La versión 4 del Protocolo de Internet es la cuarta revisión en el desarrollo del sistema de Protocolos de Internet (IP) y es la primera versión que se utiliza de forma global. Conjuntamente con la versión 6 (IPv6), está basada en los métodos estándar de Internet". Registro de Dominio, (2010). Consultado el 7 de Julio de 2010 (http://www.internetlab.es)

IPv6.-"IPv6 (también conocido como IPng o "IP de nueva generación") es la nueva versión del conocido protocolo de red IP, también llamado IPv4. Como sucede con el resto de los sistemas *BSD FreeBSD proporciona una implementación de referencia que desarrolla el proyecto japonés KAME. FreeBSD dispone de todo lo necesario para experimentar con el nuevo protocolo de red. Esta sección se centra en conseguir configurar y ejecutar correctamente el protocolo IPv6".El poder del servicio Freebsd, (1995-2012). Consultado el 2 de Febrero de 2012. (http://www.freebsd.org)

***IPsec*.-**“Es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4”. Buchen, J.(2007). Configuración *IPsec*. Consultado el 10 de Agosto del 2010. (http://www.ipsec-howto.org)

Red de datos.- “El concepto procede del latín rete y puede hacer referencia a la interconexión de computadoras y otros dispositivos que comparten recursos. Dato, del latín *datum*, es un término que indica una información, un documento o un testimonio”. Las definiciones, (2008-2011). Consultado el 4 de febrero de 2012. (http://definicion.de/red-de-datos/)

1.5.3 Marco Legal

IPv6 es un protocolo nuevo que todavía no se encuentra implementado en la mayoría de proveedores de Internet en el Ecuador, por lo que su regulación no se encuentra definida aún, pero su utilización a nivel Mundial se rige bajo los reglamentos de IANA (*Internet Assigned Numbers Authority*), Institución que se encarga de administrar la distribución de los bloques de IPv6 de acuerdo a la estructura que se rige bajo la publicación en el documento RFC 2460.

1.5.4 Marco temporal y espacial

El tiempo para la implementación se lo ha planificado empezar desde enero 2011, en el Ecuador específicamente en las ciudades de Quito, Santo Domingo, Salinas, Guayaquil, Ambato, Riobamba, Cuenca, Loja, Ibarra, Tulcán, Machala, Quevedo, Bahía de Caráquez, Puyo, Lago Agrio. Donde la Universidad Tecnológica Equinoccial posee sus campus y centros de apoyo

1.6 HIPÓTESIS

1.6.1 Hipótesis General

La red de datos en la Universidad Tecnológica Equinoccial actualmente opera con IPv4, cuyo direccionamiento IP como se ha analizado presenta limitaciones, que con el nuevo direccionamiento IPv6 se responderían a las exigencias de eficiencia, confiabilidad que el usuario necesita y exige.

1.6.2 Hipótesis Específicas

Es necesario pensar en un rediseño del proceso de direccionamiento IP, para implementar un nuevo esquema que consolide, sistematice y produzca un intercambio de información lo más confiable e inmediato, de todos los servicios que ofrece la UTE, con todos los datos en detalle, precisos y transparentes, a su personal directivo, docente, administrativo, de servicios, estudiantes y público en general.

Se asume, que es también indispensable, la implementación de un software especial y particular, y un hardware de última generación que haga posible el llevar a cabo este proceso de cambio y actualización del sistema informático

Finalmente, este probable cambio en la estructura mencionada requerirá de recursos humanos capacitados, actualizados y con la virtud de aceptar cambios y presiones en el trabajo; ya que la implementación demandará tiempo y algunas variaciones en la estructura de la red de Universidad.

1.7 VARIABLES

1.7.1 Variable Independiente

- Sistema de Direccionamiento IPv6

1.7.2 Variables Dependientes

- Optimización y Efectividad
- Ahorro financiero

1.8 ESTRATÉGIA METODOLOGÍCA.

1.8.1 Unidad de Análisis

El actual trabajo de investigación va a analizar, desarrollar e implementar IPv6 en la intranet y extranet de la Universidad Tecnológica Equinoccial.

1.8.2 Método de Investigación

Para la implementación de IPv6 se realizará una investigación que se enfocará en los métodos teóricos y empíricos basados en:

- Mediciones
- Experimentos
- Encuestas
- Análisis
- Síntesis
- Inducción
- Deducción
- Lógico

1.8.3 Métodos Teóricos

- **Método inductivo-deductivo** para analizar el problema de investigación y diseñar el sistema de direccionamiento.

- **Analítico - sintético** para estudiar las partes descomponiendo el todo y realizando los procesos inversos.

- **Método sistémico** para interrelacionar las partes del sistema tecnológico, analizar sus interrelaciones y las lógicas estructurales.

1.8.4 Métodos Empíricos

- **Revisión documental** se revisará la bibliografía especializada sobre los estándares y normas del protocolo de direccionamiento IPv6.

- **Consulta a expertos**se pedirá opiniones y criterios a varias empresas expertas que hayan usado ya este protocolo IPv6, así como de la solución tecnológica que se propone.

- **Experimentación**se verificará el funcionamiento del protocolo IPv6 y los estándares de calidad proyectados sobre el mismo. Se llevará a cabo una serie de pruebas previas antes de la implementación final del protocolo IPv6.

1.8.5 Tipo de Investigación

La Investigación que se utilizará es la exploratoria y de monitoreo de desempeño, ya que el análisis será del tipo cuantitativo y cualitativo, tomando en cuenta que la exploratoria es sugerida en el manual para una tesis de maestría.

1.8.6 Fuentes de Información

Los Datos serán obtenidos de fuentes primarias y secundarias, ya que se realizará experimentos y se recolectará datos obtenidos por otras personas, libros e Internet.

CAPITULO II

MARCO TEÓRICO

2 HISTORIA DEL INTERNET DESDE IPV4 A IPV6

El internet fue desarrollado con el afán de apoyar a las fuerzas militares en el caso de que se desatará una guerra, con el objetivo de poder comunicarse entre distintas ciudades, bases y lugares; quien diría que este suceso llevo a la creación de uno de los inventos más grandes que el hombre ha realizado y que hasta hoy es usado a nivel mundial.

Sin duda alguna la creación del internet con el fin que fuese, se ha convertido en la forma de comunicación de millones y millones de personas; tal es el caso que se lo utiliza en: hogares, oficinas, empresas, escuelas, universidades, etc.

"El Internet sea convertido en una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores independientemente de su localización geográfica."[1]

A finales de los años 60 la ARPA (Agencia de Proyectos de Investigación Avanzados) del Departamento de Defensa definió el protocolo TCP/IP(Protocolo de Control de Transmisión"TCP" y Protocolo de Internet"IP"), que serviría para enlazar diferentes computadoras que utilizan diferentes sistemas operativos sobre: PAN, LAN, WAN y MAN.

[1] http://www.maestrosdelweb.com/editorial/internethis/

En los años 70 y 80 distintos grupos sociales tenían en su poder ordenadores, los cuales comenzaron a conectarse a la gran red de redes; el TCP/IP por ser de dominio público y de fácil manejo era una gran atracción para la gente que deseaba enlazarse a esta compleja ramificación. Como en todo invento mientras más usuarios mejor, ya que se la consideraba más valiosa según abarcaba grandes extensiones de terreno, gente y recursos.

Debido al crecimiento de las redes, PC y estaciones de trabajo fue necesario crear o definir tres clases de redes A, B y C; las cuales ayudarían a acomodar las existentes. La clase A fue asignada para pocas redes con muchos ordenadores, mientras que la clase B para redes regionales y la clase C para muchas redes con relativamente pocos computadores.

A la creación de clases se le dará el nombre de IPv4, la misma que usa direcciones de 32 bits, es decir a 2^{32} = 4.294.967.296 direcciones únicas.

Actualmente hay varios miles de redes de todos los tamaños conectadas a Internet, más de seis millones de servidores y entre cincuenta millones de personas que tienen acceso a sus contenidos; y cabe destacar que estas cifras siguen creciendo día a día.[2]

Sin duda alguna la gran demanda en el uso del internet ha obligado a sus creadores, científicos y demás entendidos a buscar mejoras constantemente, es así que *Steve Deering* de Xerox PARC y *Craig Mudgehan*

[2]http://catarina.udlap.mx/u_dl_a/tales/documentos/lhr/herszenborn_m_n/capitulo2.pdf

diseñaronIPv6cuyoprincipal objetivo es proporcionar mayor número de direcciones de red, lo que facilitaría la conexión a Internet sin restricciones.

2.1 MODELOS OSI, TCP/IP E HÍBRIDO

2.1.1 Modelo OSI

A inicio del año 1980 el crecimiento y expansión de las redes fue enorme, causando un desorden en el intercambio de información; ya que existía diferencia en lo que se refiere a especificaciones e implementaciones en los equipos que formaban parte de las redes.

Conociendo este problema la Organización Internacional de Estandarización (ISO), desarrolló un conjunto de estándares que normaban la comunicación de datos; permitiendo que se cree una interconexión de sistemas abiertos es decir que la comunicación de equipos en las redes sea independiente del fabricante, sistema operativo, arquitectura, etc.

El modelo de referencia OSI (*Open SystemInterconnection*) está constituido por siete niveles, los mismos que contienen normas que cada nodo debe seguir para poder intercambiar información libremente independiente de los sistemas o suplidores.

OSI posee un modelo en el cual cada nivel tiene un protocolo con funciones específicas para comunicarse con el nivel de la capa superior o inferior.

2.1.1.1 Capas del Modelo OSI

El Modelo de Referencia Interconexión de Sistemas Abiertos (OSI), contiene siete capas o niveles; a continuación una breve descripción de cada uno de ellos:

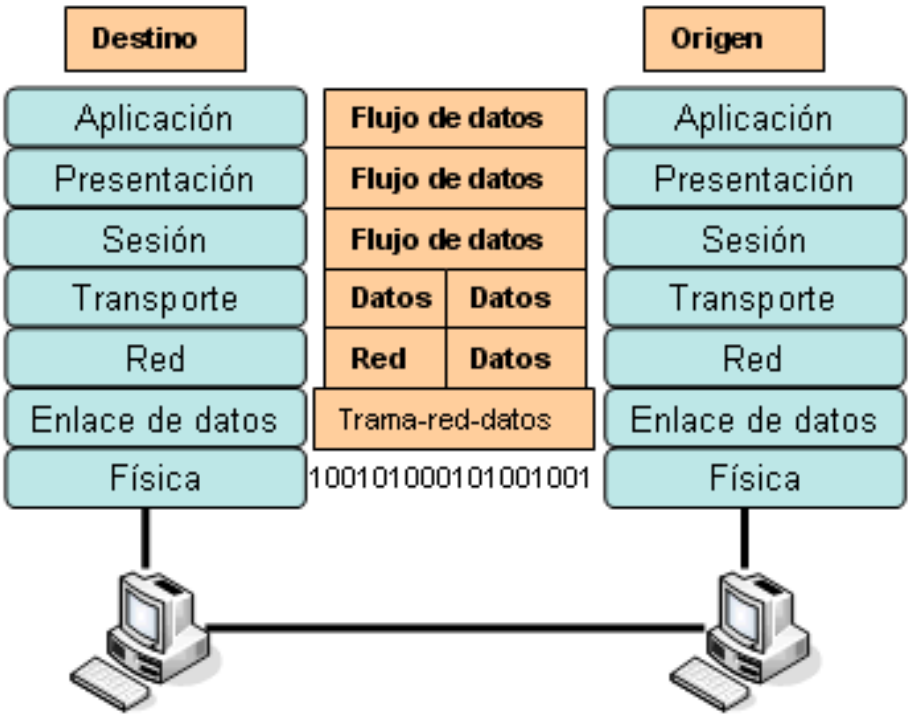

Figura 2-1. Las 7 capas de modelo OSI
Fuente: ADR Infor S.L.,www.adrformacion.com/cursos/wserver/leccion1/tutorial4.html
Elaborado por: El Autor

a) Capa 1 Física

La tarea de esta capa es controlar la transferencia de datos en forma binaria entre los diferentes puntos, tomando en cuenta velocidad y tipo de transmisión, determinar si la conexión es punto a punto o multipunto; así como también define la interfaz, terminales, equipos, etc.

En la capa o nivel físico se establece el medio de comunicación que será utilizado para la transferencia de la información.

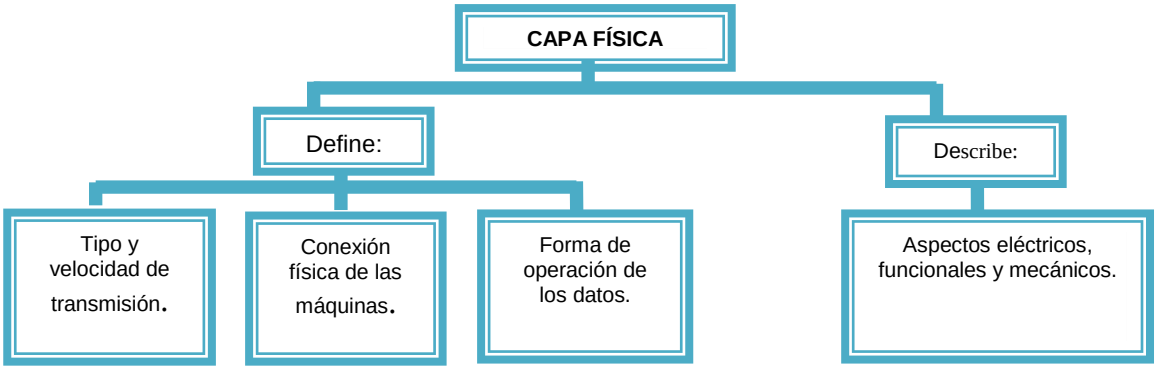

Figura 2-2. Capa Física Modelo OSI
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

b) Capa 2 de Enlace de datos

El objetivo principal de esta capa es verificar que no existan fallas en la transferencia de datos, proporcionando al próximo nivel una transmisión libre de errores. Para lograr este propósito se emplea el Chequeo de Redundancia Clínica (CRC).

En esta capa se organizan los 1L y los 0L en grupos lógicos de información, permitiendo establecer el método de acceso para el envío y recepción del mensaje, así como también se determina si la transferencia es sincrónica o asincrónica.

Se utilizan protocolos como: BSC (*BinarySynchronousCommunication*, HDLC (*High Level Data Link Control*), SDLC (*Synchronous Data Link Contro*l), DDCMP (*Digital Data Communication Message Protocol*).

c) Capa 3 de Red

La capa de red es la encargada de establecer, mantener y terminar la conexión de la red. Define si un mensaje está listo para ser enviado a la siguiente capa o si debe volver a la capa de Enlace y ser revisado nuevamente.

Se podría definir como un semáforo el cual está controlando la congestión de los paquetes de información, especificando la vía más adecuada dentro de la red para establecer la comunicación. Realiza la determinación de la mejor ruta.

d) Capa 4 de Transporte

En algunos libros se lo denomina como un puente entre los niveles inferiores y superiores, ya que tiene la función de garantizar una entrega de información libre de erros, en secuencia y sin perdidas de información.

En la capa de transporte se segmenta los mensajes en pequeños paquetes para ser enviados y luego se re ensamblada en los host destinatarios.

Proporciona el control de flujo entre los diferentes host y efectúa una conexión de extremo a extremo.

e) Capa 5 de Sesión

Posee características similares a la capa de transporte, pero se adicionan otros servicios, como por ejemplo: puntos de chequeo o verificación (garantiza que si existe una interrupción en la transmisión de datos, estos se recuperen desde el último punto de verificación.), organización y sincronización de transferencia e intercambio de datos.

Se realiza la comunicación entre los diversos dispositivos de la red y se asegura que la sesión establecida entre máquinas se ejecute de principio a fin.

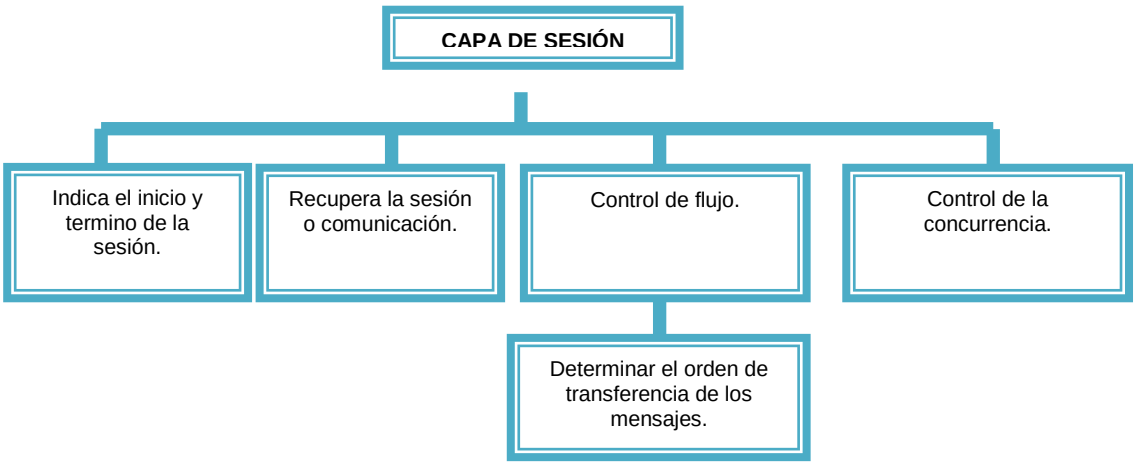

Figura 2-3. Capa Sesión Modelo OSI
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

f) Capa 6 de Presentación

Se realiza un trabajo más directo con lo que se refiere a información, es decir que en esta capa se efectúa la representación de datos; de tal forma que se traduce el formato a uno de sintaxis reconocible para todos los que intervienen en la comunicación.

A continuación se puede apreciar un mapa conceptual de algunos de los diferentes formatos o representaciones internas que un equipo puede tener.

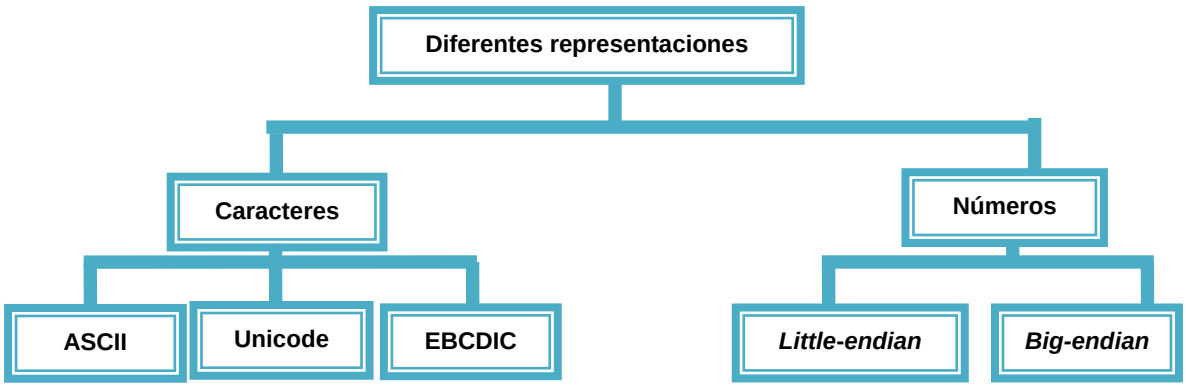

Figura 2-4. Capa de presentación y sus representaciones numéricas
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Como se puede apreciar en esta capa ya no se pone mayor interés en la comunicación.

g) Capa 7 de Aplicación

En esta última capa del modelo OSI se establece o define los protocolos mediante los cuales las aplicaciones procederán a realizar la transferencia e intercambio de datos.

Existe importante mencionar que todo el proceso de transferencia de datos no se lo realiza directamente entre el usuario y la capa de aplicación, sino que el usuario interactúa con programas que a su vez se comunican con la capa de aplicación; es decir que existe una interfaz para el usuario (la misma que entrega y recibe información o comandos que permiten la comunicación).

2.1.2 Modelo TCP/IP

El modelo TCP/IP es muy similar al modelo de referencia OSI,ya que tiene la función de estandarizar la comunicación de equipos; haciendo posible la transferencia de información entre sí independientemente de la incompatibilidad del hardware o software de los diferentes ordenadores conectados a Internet.

2.1.2.1 Capas del Modelo TCP/IP

A diferencia del modelo OSI el TCP/IP posee cinco capas, que son: **física, enlace, red, transporte y aplicación**. En algunas fuentes de consulta se ha encontrado que el TCP/IP posee cuatro, debido a la fusión entre la capa física y la de enlace definiendo así la capa **acceso de red**.

A continuación una descripción de cada una de estas capas.

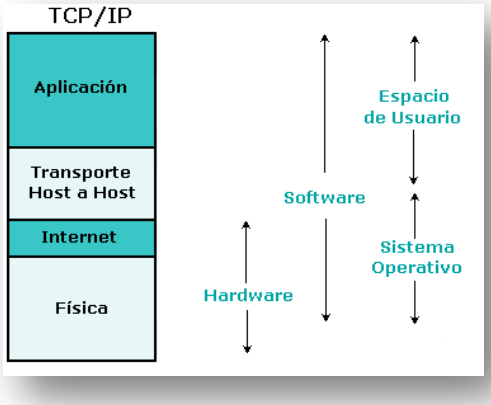

Figura 2-5. Capas Modelo TCP/IP
Fuente: Universidad Industrial de Santander,http://ocw.uis.edu.co/tecnologias-de-informacion-y-comunicacion-tics/tcp-IP/InternetProtocolosServicios/imagenes/tcp_IP_osi.gif
Elaborado por: El Autor

a) Capa 1 Física

Se puede definir como similar a la capa física del modelo OSI, es decir controla la transferencia de datos en forma binaria entre los diferentes puntos.

b) Capa 2 de Internet

Se verifica los datos(o identificación) de la máquina destino, y se valida los datagramas que deben ser enviados; si todo está correcto se procede a utilizar un algoritmo de ruteo (determina si se procesa de manera local o transmitida) para el envió de información y comunicación con la otra máquina. En la capa Internet se emplea el protocolo IP.

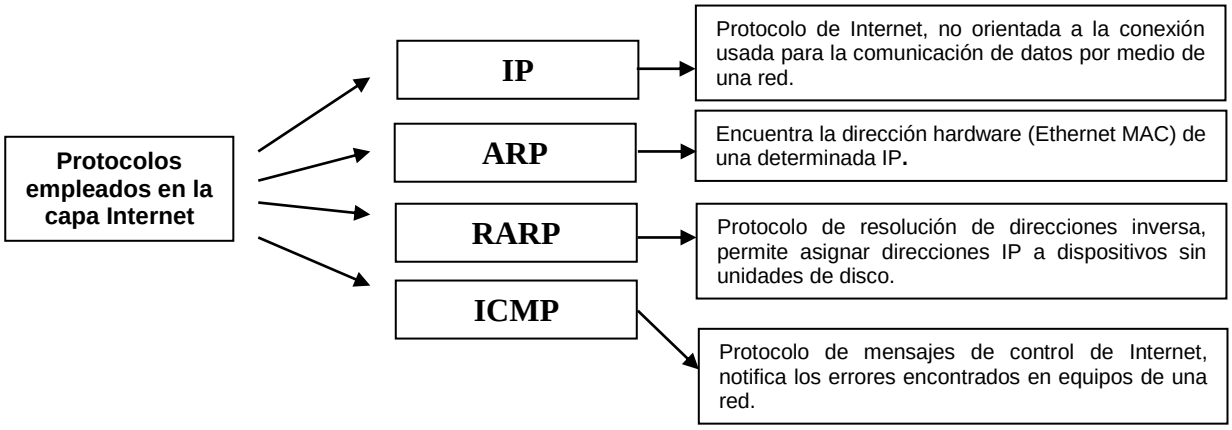

Figura 2-6. Protocolos Capa Internet
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

c) Capa 3 de Transporte

La capa de transporte está encargada de verificar que los datos enviados se dirijan al destino correcto, se establece una conexión entre el emisor y receptor validando así que la información sea la adecuada; caso contrario se vuelve a solicitar el dato.

En esta capa se encuentran o utilizan los protocolos TCP y el UDP[3].

d) Capa 4 de Aplicación

El modelo TCP/IP tiene en el nivel superior a la capa de aplicación, dentro de la cual se encuentran protocolos como: TELNET (admite que un usuario mediante una red acceda a otra máquina virtual y trabaje ahí), FTP (Protocolo de Transferencia de Archivos, transfiere datos de una máquina a otra), SMTP (Protocolo Simple de Transferencia de Correo, utilizada para el intercambio de correo electrónico).

2.1.3 Modelo Híbrido

Según el libro de Redes de Computadores de Andrew Tanenbaum (Sexta Edición 1996) el modelo híbrido no es más que la fusión entre el Modelo OSI y el TCP/IP, en el cual se toma lo mejor de los dos modelos antes mencionados.

2.2 ORGANISMOS DE CONTROL Y ASIGNACIÓN DE DIRECCIONES IP

Antes de conocer los organismos de control que permiten la asignacion de direcciones IP, es necesario saber que tipos de direcciones existen.

2.2.1 Tipos de direcciones IPv4

Las direcciones IP constan de números binarios de 32 bits que son asignados a los host mediante el protocolo IPv4.

---

[3] http://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/udp.html

Existen tres tipos de direcciones IP.

- Direcciones IP públicas
- Direcciones IP privadas
- Direcciones IP especiales y reservadas

2.2.1.1 Direcciones IP públicas

Son asignadas para ser globalmente utilizadas, son únicas y cuando un computador tiene una IP pública es accesible desde cualquier otro ordenador. Usualmente un host debe tener una dirección IP pública para poder conectarse a Internet.

2.2.1.2 Direcciones IP privadas

Son rangos de direcciones IP asignadas para funcionamiento de redes privadas. Estas direcciones pueden ser utilizadas por cualquier organización sin solicitar ningún Registro de Internet.

2.2.1.3 Direcciones especiales y reservadas

Se denominan direcciones IP especiales y reservadas aquellas que se utilizan para asignar: direcciones de red (se obtiene cuando los bits reservados para los equipos de red es reemplazado por cero), dirección del equipo (se reemplaza por cero los bits asignados para el identificador de red), dirección de difusión (cuando los bits de identificación de equipos de red son reemplazados por uno), dirección de multidifusión(se reemplaza por uno los bits de identificación de red) y dirección de bucle de retorno(indica el host local **127.0.0.1**).

2.2.2 Principales Organismos para la asignación de direcciones IP

A pesar de que el uso del Internet es global y puede ser accedido libremente, existen organismos que regulan y controlan aspectos como asignación de direcciones, dominios, parámetros del TCP/IP, etc. Esto permite que los usuarios no puedan realizar modificación en los servidores raíces, evitando por ejemplo: que se cambie un pointer ".es", ".ar", ".com", etc.

Los organismos que se verán a continuación tienen como objetivo distribuir las direcciones IP brindando a sus usuarios finales exclusividad, conservación, ruteabilidad y registro.

Tabla 2-1. Organismos para la asignación de direcciones IP

ORGANISMO	FUNCIONAMIENTO
IANA*(Autoridad de Asignación de Números en Internet)*	Antiguamente era el organismo que tenía la autoridad para asignar el uso de las direcciones IP sobre todo el mundo, fue reemplazado en 1998 por la ICANN.
ICANN(*Corporación de Internet para la asignación de Nombres y Números*)	Se encarga de algunas tareas que realizaba el IANA, tales como: Gestionar la asignación de direcciones IP, nombres de dominio, gestionar los servidores raíz y parámetros relacionados con el Protocolo TCP/IP. Fue creada el 18 de septiembre de 1998.
RIR*(Registro de Internet Regional)*	Para un mejor manejo del Internet, se crea delegaciones encargadas de supervisar la asignación de direcciones IP que se encuentran divididas según las regiones o continentes, dentro de las cuales se puede mencionar: **ARIN** (para América del Norte), **RIPE NCC** (Europa, el Oriente Medio y Asia Central), **APNIC** (Asia y la Región Pacifica), **LACNIC** (para América Latina y el Caribe) y **AFRINIC** (para África).
ISP*(Proveedores de Servicios de Internet)*	Un proveedor de internet está encargado de dar direcciones IP a sus usuarios finales, así como también dar mantenimiento para que el acceso al Internet sea correcto. Otra de sus facultades es la de ofrecer registros de dominio, almacenamiento de información, imágenes, videos, etc. mediante la vía Web.

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado Por: El Autor

Al final de cada una de estas organizaciones se encuentran los usuarios finales denominados también "UF", los mismos que harán uso de las direcciones IP.

2.2.2.1 Objetivos de la asignación de direcciones IP públicas.

La asignación de direcciones IP debe garantizar lo siguiente: exclusividad, conservación, *ruteabilidad* y registro.

- **Exclusividad:** se refiere a que cada host o dispositivo en la Internet tenga una dirección IP irrepetible, garantizando que se pueda identificar de forma única alrededor del mundo y de la red en la que se encuentra.
- **Conservación:** con el objetivo de no desperdiciar las direcciones IP, se distribuye de manera exacta a los usuarios finales las direcciones que cada uno necesita.
- ***Ruteabilidad*:** asignación de direcciones IP según una jerarquía, obteniendo un adecuado funcionamiento dela Internet.
- **Registro:** permite manejar una documentación sobre la asignación de direcciones IP realizadas.

2.3 MODELO TCP/IP HACIA IPV4

El denominado Protocolo de Control de Transmisión/Protocolo de Internet TCP/IP se encuentra divido en cinco capas, las cuales se hallan una a continuación de otra. La tarea de cada capa se la efectúa secuencialmente, se envía los datos o el paquete de información más un encabezado identificador.

El TCP/IP se asegura de proporcionar una conexión lógica fiable, por lo que suministra servicios a las aplicaciones que utiliza.

2.3.1 FORMATO DE SEGMENTO TCP/IP Y UDP

El formato de segmento agrupa a los datos y les agrega un encabezado, permitiendo sincronizar las transmisiones y garantizar la recepción del mensaje.

En la figura 2.7 se puede observar cómo se encuentra estructurado el segmento TCP/IP.

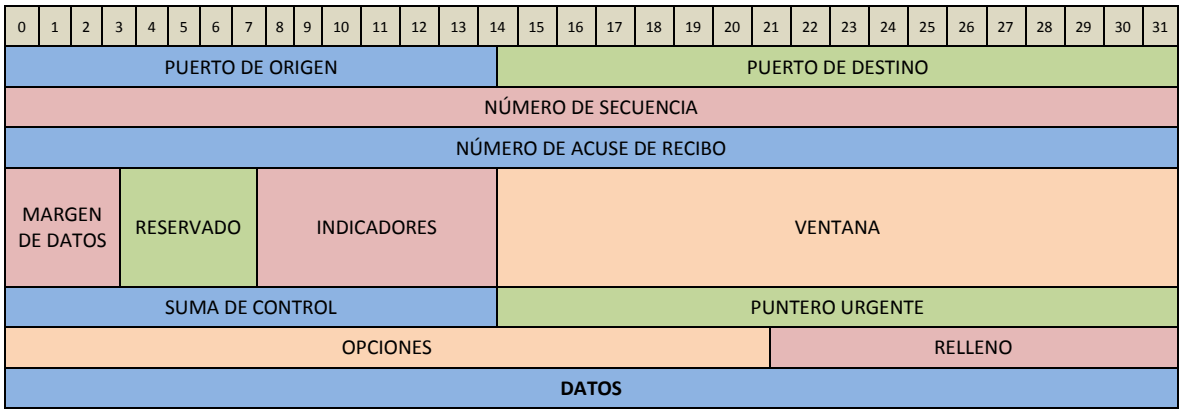

Figura 2-7. Formato de segmento TCP/IP
Fuente: Computing community, http://es.kioskea.net/contents/internet/tcp.php3
Elaborado por: El Autor

La función que cada campo del segmento TCP/IP realiza se detalla a continuación:

- **Puerto de origen:** utiliza 16 bits y está relacionado con la aplicación ejecutante en la máquina origen.
- **Puerto de destino:** emplea 16 bits y está relacionado con la aplicación ejecutante en la máquina destino.
- **Número de secuencia:** trabaja con el indicador SYN y utiliza 32bits. Si el SYN se encuentra en estado 0, el número de secuencia es igual a la primera palabra del segmento enviado; si el indicador se encuentra en 1 el número de secuencia es igual a la secuencia inicial que se empleó para sincronizar el ISN.

- **Número de acuse de recibo:** se encuentra relacionado con el número de secuencia del último segmento esperado y emplea 32 bits.

- **Margen de datos:** 4 bits para identificar el inicio de los datos en el paquete.

- **Reservado:** se ha asignado 6 bits para este campo, actualmente no está en funcionamiento y se espera usarlo en el futuro.

- **Indicadores:** el papel de los indicadores es entregar información adicional de la importancia que tiene el envío del paquete, así como también si ha existido una interrupción o restablecimiento de conexión. Posee 6 bits y dentro de los indicadores se pueden mencionar:

  - **URG.-** si el estado del indicador es 1, el paquete debe ser procesado de forma urgente.

  - **ACK.-** si su estado es 1, el paquete se asigna como **acuse de recibo.**

  - **PUSH.-** el funcionamiento de este indicador está relacionado con el método PUSH.

  - **RST.-** este indicador trabajo con estado 1 e indica el restablecimiento de la conexión.

  - **SYN.-** mediante este indicador se efectúa el pedido de establecer una conexión.

  - **FIN.-** si su estado es 1, se interrumpe la conexión.

- **Ventana:** campo con 16 bits, sin necesidad de **acuse de recibo** permite conocer la cantidad de bytes que el receptor tiene que recibir.

- **Suma de control:** tomando la suma del campo de datos del encabezado se comprueba que este se encuentre integro (sin daños o pérdidas de información).Para este campo se asigna 16 bits.

- **Puntero urgente:** en el caso de existir una petición del indicador como paquete a procesar de forma urgente, se indica el número de secuencia después del cual la información será tomada como urgente. La asignación para este campo es de 16 bits.
- **Opciones:** posee un tamaño variable y puede ser empleado para diferentes opciones.
- **Relleno:** es un espacio restante después de **opciones.**

El último y más importante Datos**,** que es la información que debe ser enviada al receptor.

2.3.2 DESCRIPCIÓN DEL UDP

El UDP (Protocolo de Datagramas de Usuario) es considerado como una interfaz de aplicación para IP, en la práctica no tiene tanto uso como TCP/IP ya que no soporta control de flujo, recuperación de errores y confiabilidad para IP.

El UDP actúa simplemente como un multiplexor que permite enviar y recibir datagramas por medio de puertos. Para el envío y recepción de datagramas utiliza una aplicación, la misma que deberá realizar la recuperación de errores y demás características que UDP no posee.

2.3.2.1 Formato del datagrama UDP

Como se mencionó anteriormente para que un UDP funcione necesita una aplicación, la cual deberá estar diseñada para aceptar datagramas de 576 bytes, con cabeceras de máximo 60 bytes. En el caso del Protocolo de Datagramas de Usuario se utiliza 16 bytes para la cabecera, su descripción se muestra a continuacion.

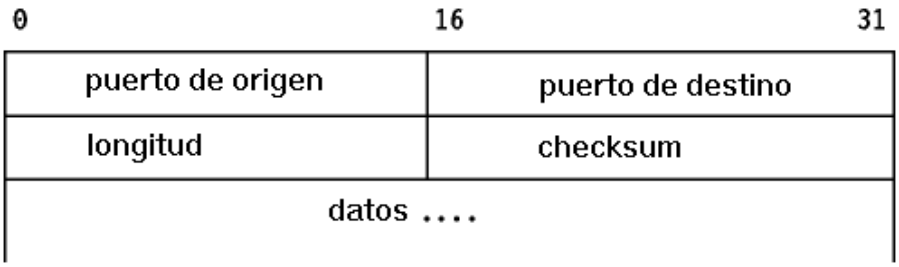

Figura 2-8. Formato de cabecera UDP
Fuente: http://personales.upv.es/rmartin/TcpIp/cap02s11.html
Elaborador por: El Autor

- **Puerto de origen:** hace referencia al número de puerto que envía el datagrama.

- **Puerto de destino:** indica el número de puerto del host destino.

- **Longitud:** se refiere al tamaño en bytes del datagrama (incluida la cabecera).

- **Checksum:** es un complemento a la cabecera pseudo IP, la cabecera y los datos tienen asignados 16 bits.

La cabecera pseudo – IP está compuesta de la dirección IP origen y destino, un campo protocolo y la longitud UDP como se muestra en la Figura 2-9.

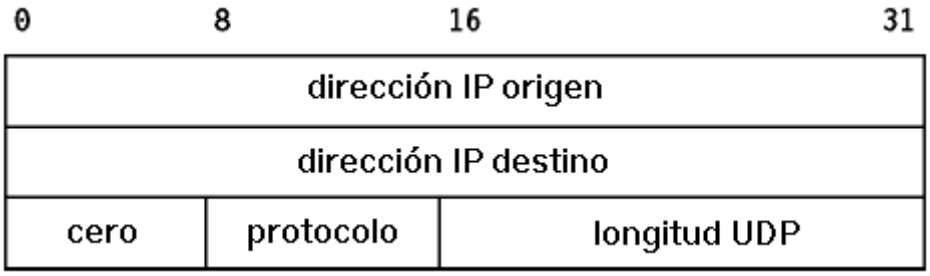

Figura 2-9. Formato de cabecera UDP
Fuente: http://personales.upv.es/rmartin/TcpIp/cap02s11.html
Elaborado por: El Autor

2.3.3 DATAGRAMA Y TRAZA IP

UDP, IPX, IP o AC y CL utilizan o se refieren a los datagramas como un fragmento de mensaje (empaquetado) que se envía a un determinado host destino, con la respectiva estructura es decir una cabecera y los datos.

Cada datagrama es enviado por medio de la red a su equipo receptor sin garantizar que el paquete llegue en el orden adecuado.

Como se puede observar en la siguiente figura2.10los datagramas deben recorrer o realizar algunas etapas antes de llegar a su host destino, como por ejemplo: primero se debe establecer una conexión con el receptor, segundo definir qué ruta va a tomar y finalmente entregar el datagrama al destino.

Para la entrega de un datagrama no siempre se sigue la misma ruta, aun cuando el host destino sea el mismo.

La Figura.2-10 muestra como una máquina origen desea enviar un datagrama o paquete de información a una máquina destino, pero para ello define que el datagrama será enviado pasando por el *router* 2.

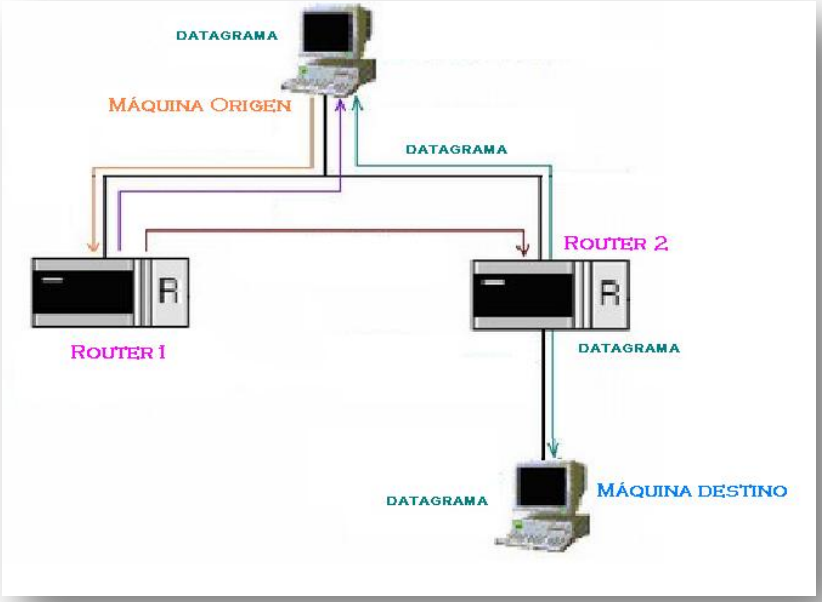

Figura 2-10. Envío datagrama
Fuente: http://personales.upv.es/rmartin/TcpIp/cap02s11.html
Elaborado por: El Autor

Para poder establecer una conexión entre diferentes máquinas es necesario conocer la MAC (Media Access Control) de cada host, esta acción se la realiza empleando los protocolos ARP (*Address Resolution Protocol*) y RARP (*Reverse Address Resolution Protocol*). A continuación la descripción de estos protocolos.

2.3.4 PROTOCOLO ARP

Conocido también como protocolo de resolución de direcciones, para el envío y recepción de datagramas, para establecer una conexión, para identificar a un host, son entre otras las acciones que este protocolo permite realizar.

El ARP se encarga de encontrar la MAC (Control de Acceso de Medio) de una dirección IP, lo que permite identificar a una máquina; para realizar este proceso se envía un ARP *request* a la dirección IP por la que se pregunta, la máquina cuya dirección IP sea la solicitada envía un ARP *reply* con la respectiva dirección Ethernet.

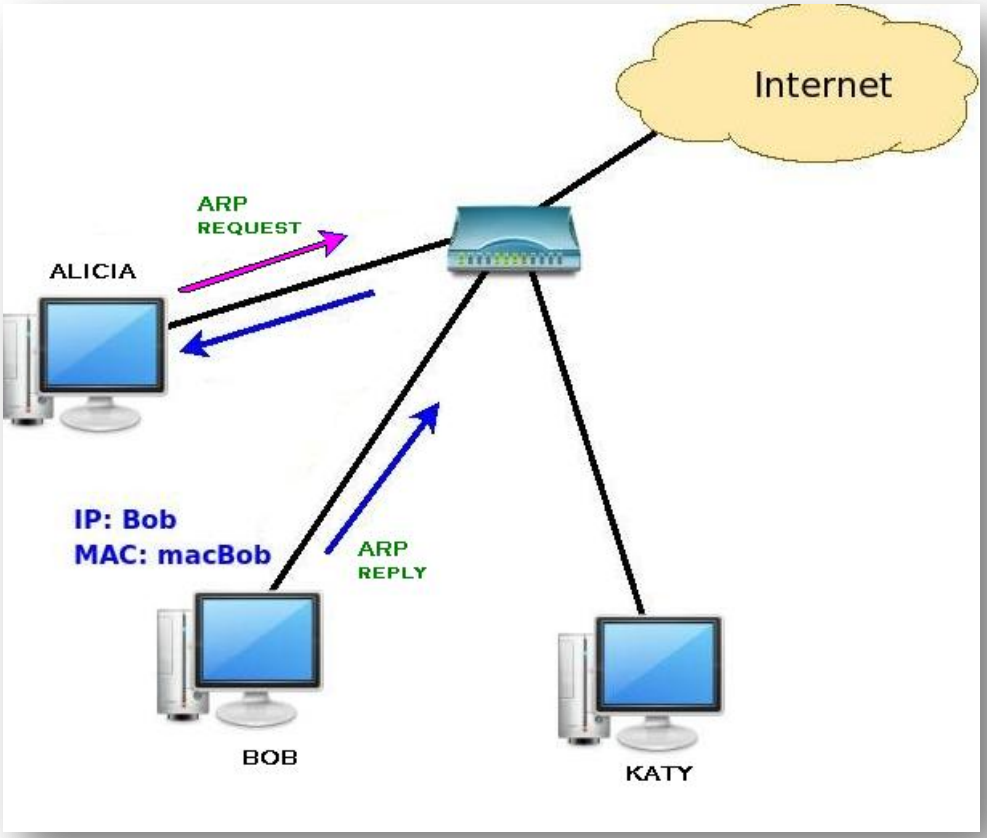

Figura 2-11. Protocolo ARP
Fuente: http://joanps.freehostia.com/images/a3/Diagram3.jpg
Elaborado por: El Autor

El ARP se utiliza cuando dentro de una misma red dos host desean intercambiar información, así como también cuando un *router* desea enviar un paquete a un host o a otro *router*, etc.

2.3.5 PROTOCOLO RARP

A diferencia del ARP este protocolo se encarga de entregar la dirección IP de una MAC. Sus siglas RARP son definidas como Protocolo de Resolución de Direcciones Inverso.

El RARP es empleado cuando se desea conocer la dirección física de una máquina sin disco.

Tabla 2-2. Diferencias ARP y RARP.

ARP	RARP
Entrega la dirección MAC de una IP	Entrega la dirección IP de una MAC
La búsqueda de la MAC es automática	El administrador debe definir los parámetros de la búsqueda.
No requiere mucho tiempo de administración.	La búsqueda debe ser actualizada y necesita mucho tiempo de administración.

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: Autor de la tesis

En la Tabla 2-2 se puede apreciar las diferencias entre los protocolos ARP y RARP, llegando a la conclusión que cada uno de ellos efectúa una función completamente diferente.

El RARP requiere mayor tiempo de administración para la actualización de las tablas de búsqueda.

2.4 PROTOCOLO IPV6

El protocolo **IPv6** se ha diseñado con el propósito de reemplazar al actual uso de IPv4RFC 791, ya que como se ha mencionado anteriormente presenta ciertas limitaciones para la demanda actual dela Internet.

Dentro de la limitación más importante que se puede mencionar de IPv4 está el tamaño de direcciones que se asigna a los usuarios del Internet.

Debido al crecimiento poblacional se ha visto la necesidad de restringir su asignación; pues se considera que las dos terceras partes de direcciones ya han sido asignadas.

Steve Deering (Xerox) y Craig Mudge con la firme convicción de solucionar y mejorar las limitantes actuales de IPv4 diseñan a IPv6 que posibilita asignar 670 mil billones de direcciones/mm^2 de la superficie de La Tierra.[4]

IPv6 ha mantenido las principales características de IPv4, mejorando y removiendo aquellas que son poco utilizadas y se encuentran desperdiciadas. Además se considera que IPv6 evoluciona notablemente respecto a IPv4.

2.4.1 CARACTERÍSTICASIPv6

Los cambios de IPv4 a IPv6 se caracterizan de acuerdo a los siguientes aspectos:

[4] http://es.wikipedia.org/wiki/IPv6

2.4.1.1 Incremento de direccionamiento

IPv6 aumenta el tamaño de dirección IP de 32 bits a 128 bits, lo que permite una autoconfiguración más simple de direcciones y garantiza que cada dispositivo conectado a la red tenga una dirección IP pública.

Se define un nuevo tipo de direccionamiento denominado "dirección envío a uno dé", usado para enviar un paquete a cualquiera de un grupo de nodos.

2.4.1.2 Formato de cabecera

Aquellos campos de la cabecera IPv4 que en la práctica no han sido usados se han eliminado, simplificando el manejo de paquetes y reduciendo el costo de procesamiento de los mismos.

2.4.1.3 Mejora en el reenvió de paquetes

El mejoramiento de la cabecera IP permiten un reenvío más eficiente, con ahorro en el ancho de banda.

IPv6 incorpora cabeceras adicionales, que en el futuro darán una mayor flexibilidad para introducir nuevas direcciones o expandirse.

2.4.1.4 Etiquetado de flujos

IPv6 permitir el etiquetado de paquetes, de tal manera que se puede tener un tratamiento especial en el envío y recepción.

2.4.1.5 Autenticación y Privacidad

IPv6 incluye la especificación de extensiones que proveen autenticación, integridad, y (opcionalmente) confidencialidad de los datos[5].

2.4.2 DIRECCIONAMIENTO IPv6

IPv6incrementa la longitud de las direcciones de red a 128 bits, aproximadamente 3.4×10^{38}. Este número puede también representarse como 16^{32}, con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores.

2.4.2.1 Mecanismos de configuración de direcciones

Un host se puede configurar en IPv6 de tres distintas formas:

- Estática
- Autoconfiguración sin estados
- DHCPv6 (Dynamic Host Configuration Protocol).

Estática

La configuración estática al igual que IPv4consiste en ingresar manualmente la dirección IPv6 o mediante comandos propios del sistema operativo que soporte IPv6.

[5] http://es.wikipedia.org/wiki/IPv6

Autoconfiguración sin estados (*stateless)*

La autoconfiguración sin estados a través del protocolo de descubrimiento de vecinos (NDP) y crear una dirección IPv6 a partir delos prefijos de la siguiente forma:

- **Identificar un prefijo utilizado en el enlace**: a través de los mensajes RA[6] el host escucha los anuncios que envían los *routers* periódicamente al enlace, y a partir del RA obtiene la información del prefijo de red.
- **Crear un identificador de interfaz**: El host genera un identificador de interfaz a partir de su dirección MAC (como en las direcciones locales al enlace) o de forma aleatoria.
- **Chequear que la dirección no esté duplicada**: La dirección IPv6 generada debe ser única, por lo que el nodo inicia el procedimiento de detección de direcciones duplicadas (DAD). Si la dirección es única, el nodo comienza a utilizarla.

Autoconfiguración con estados (DHCPv6)

El servicio DHCP (*Dynamic Host Configuration Protocol*) para IPv6 (DHCPv6) realiza las mismas funciones que DHCP en IPv4. Un servidor envía mensajes que contiene la dirección IPv6 a utilizar, dirección del servidor DNS (*Domain Name System*).

---

[6] ***RouterAdvertisement*(RA):** Mensaje de respuesta enviado por los router ante ***RouterSolicitation*(RS**) mensajes enviados por una interfaz activa.

El uso de DHCPv6 permite centralizar toda la asignación de direcciones de los equipo pertenecientes a un sitio.

En el cuadro se observan las principales diferencias entre DHCPv4 y DHCPv6.

Tabla 2-3. Diferencias entre DHCPv4 y DHCPv6

Característica	DHCPv4	DHCPv6
Mensaje de reconfiguración	No disponible	Permite a los servidores solicitar a los clientes que actualicen su información.
Dirección de destino de un cliente	Dirección *Broadcast*	Grupo *multicast*
Dirección de origen en la solicitud DHCP.	0.0.0.0	Dirección local de enlace del nodo
Asociación de identidad	No disponible	Los clientes pueden solicitar información a varios servidores DHCPv6 y obtener múltiples direcciones
Etiqueta de configuración asistida	No disponible	Un "*router*" puede anunciar a los nodos si es que está permitido el uso de DHCPv6.

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

2.4.2.2 Tipos de direcciones IPv6

En IPv6 se han definido los siguientes tipos de direcciones:

Tabla2-4. Tipos de Direcciones IPv6

Tipo de Dirección	Descripción
Unicast	Dirección que identifica a un host o nodo único.
Multicast	Dirección que identifica a un grupo de hosts, si se envía un paquete a una dirección *multicast*, esta se reenvía a grupo de hosts pertenecientes a ese grupo
Anycast	Dirección que identifica a un grupo de nodos, para este caso si se envía un paquete a una dirección *anycast*, es enviado al grupo o nodo más cercano del origen.

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En IPv6 se han eliminado las direcciones de *broadcast* (difusión de paquetes a todos los nodos), reemplazando su uso por las direcciones *multicast* que envían los paquetes solamente a un grupo definido.

2.4.2.2.1 Unicast

Las direcciones "*unicast*" identifican a cada nodo conectado a una red, estableciendo conexiones punto a punto entre los nodos pertenecientes a ella.

Los contextos definen el dominio de una red, por ejemplo a un nivel de directorio activo o servidor de nombres (DNS). Esta característica de reconocer el contexto al que pertenece una determinada dirección IPv6permite optimizar el manejo de los recursos de la red.

En IPv6, las direcciones *unicast* pueden pertenecer a uno de los tres contextos existentes:

Tabla 2-5. Direcciones *Unicast* de acuerdo al contexto

Contexto de las direcciones Unicast	Descripción
Local al enlace (link-local)	Identifica a todos los nodos de un enlace
Local único (unique-local)	Identifica a todos los dispositivos de una red Interna, en la que existen varios enlaces y dominios
Global	Identifica a todos los dispositivos descubiertos en la red Externa o Internet

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En IPv6 una interface puede manejar más de una dirección IP, una local al enlace (*link-local*) para comunicarse entre hosts o dispositivos locales y una global para comunicarse hacia red externa o Internet.

2.4.2.2.2 Direcciones locales de enlace (*link-local*).

Las direcciones “unicast” locales al enlace son aquellas que permiten la comunicación interna y sólo son válidas al interior del enlace.

Cuando un host inicia o se conecta a una redIPv6, se auto asigna una dirección local al enlace, basada en un identificador de interface que se genera automáticamente a partir de la dirección MAC.

En la Figura 2-12 y Tabla 2-6, a partir de la dirección MAC se detalla cómo se crea el identificador de Interface.

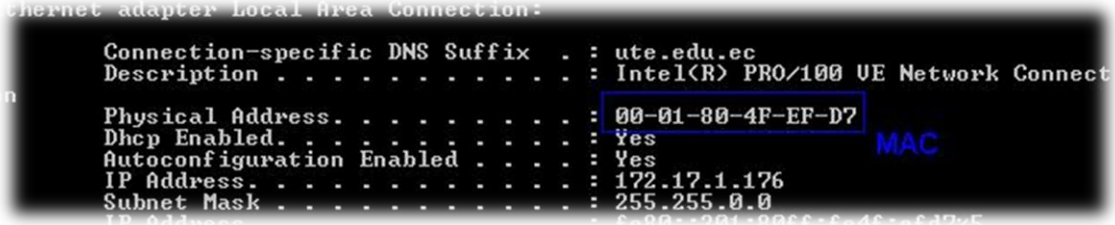

Figura 2-12. Dirección MAC; capturada de hosts
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Tabla 2-6. Generación del Identificador de interface

00	01	80	4F	EF	D7	Dirección MAC (48 Bits hexadecimales
00000000	00000001	10000000	01001111	11101111	11010111	

00000000	00000001	10000000			01001111	11101111	11010111	Extender la dirección MAC
00000000	00000001	10000000	11111111	11111110	01001111	11101111	11010111	Agregar en el medio la secuencia FF FE
00000010	00000001	10000000	11111111	11111110	01001111	11101111	11010111	Del primer octeto cambiar el bit 7 a 1
02	01	80	FF	FE	4F	EF	D7	Nuevo valor hexadecimal
0201:80FF:FE4F:EFD7								Identificador de Interface IPv6

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

2.4.2.2.3 Direcciones locales únicas (*unique-local*).

Las direcciones locales únicas permiten la comunicación al interior de toda red de una organización, de prefijo /48, compuesta por una o más subredes.

Son algo parecidas a las direcciones privadas en IPv4 y no pueden ser enrutadas hacia Internet.

Tabla 2-7. Dirección IPv6 local única

8 bits	40 bits	16 bits	64 bits
fc	Identificador único	ID Subred	ID Interface

- **fc.-** todas las direcciones se encuentra en el rango dado por el prefijo fc00::/8
- **Identificador único.-** es un valor que identifica un sitio en particular, es comparado con las direcciones reservadas en IPv4.
- **Identificador de subred.-** permite crear un plan de direccionamiento jerárquico identificando a cada una de las 400 mil posibles subredes en una organización.
- **Identificador de Interface.** Individualiza a una interface presente en una determinada subred del sitio.

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

2.4.2.2.4 Direcciones globales

Las direcciones *unicast* globales son direcciones públicas que permiten la comunicación en el Internet.

El espacio reservado actualmente para este tipo de direcciones es:

2001:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff (2001::/3)

Las direcciones *unicast* globales tienen un prefijo de red igual a /64.

Tabla 2-8. Dirección IPv6 local única

48 bits	16 bits	64 bits
Prefijo de enrutamiento	ID Subred	ID Interfaz
• **Prefijo de enrutamiento e ID subred.-**64 bits que corresponden al identificador de red. • **ID Interfaz.-** 64 bits que corresponden a la identificación de la interfaz de un nodo.		

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los primeros 64 bits (los primeros cuatro campos en formato hexadecimal) corresponden al identificador de red, y los siguientes corresponden a la identificación de la interfaz de un determinado nodo.

El prefijo de enrutamiento global de 48 bits, identifica un sitio conectado a Internet, este prefijo sigue una estructura jerárquica que tiene como objetivo reducir el tamaño de la tabla de enrutamiento, esta estructura jerárquica se puede observar en la Figura 2-13.

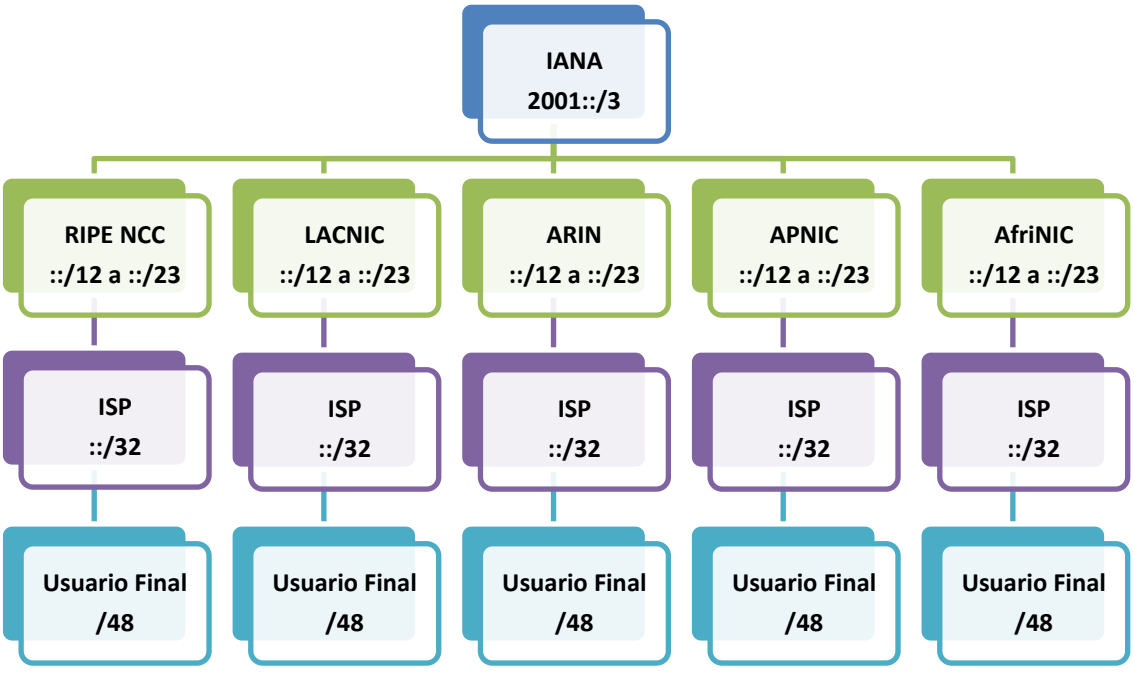

Figura 2-13. Jerarquía de asignación de prefijos de direcciones *unicast* globales
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

De acuerdo a esta estructura jerárquica, IANA como el organismo de primer nivel, entrega el total de direcciones globales *unicast*, a cada registro regional (RIR) para que manejen un prefijo /23, y estos a su vez entregan prefijos /32 a los proveedores de servicios de Internet (ISP), y los usuarios finales mantienen un prefijo /48 asignados por estos ISP.

El prefijo /48 da la posibilidad al usuario final de tener un sitio o intranet compuesto por 2^{16} subredes, y cada subred con 2^{64} hosts conectados a Internet.

2.4.2.2.5 *Multicast*

Las direcciones "*multicast*" en IPv6 tiene el mismo concepto que IPv4 y su estructura se indica en la Tabla 2-9.

Tabla 2-9. Estructura de Direcciones *Multicast*

16 bits			112 bits
FF	L	S	Identificador *multicast*

- **L**.- Indica de vida de un grupo *multicast*. 0 grupo permanente y 1 grupo temporal
- **S**.- Valor hexadecimal (4 bits) que indica el contexto del grupo de acuerdo a los siguientes valores.

Valor de S (HEX)	Contexto del Grupo
1	**Interfaz**
2	**Enlace**
5	**Sitio**
8	**Organización**
E	**Global**
Otros Valores	**Sin asignar o reservado**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Las direcciones *multicast* permiten hacer una selección más precisa de los destinatarios, evitando sobrecarga de mensajes en redes de muchos nodos. Las direcciones que identifican algunos grupos *multicast* se presenta en la Tabla 2-10.

Tabla 2-10. Direcciones de grupos *"multicast"* fijos.

Dirección *Multicast*	Detalle
FF01::1	**Todos los nodos en la Interfaz**
FF02::1	**Todos los nodos en el enlace**
FF01::2	**Todos los *router*s en la Interfaz**
FF02::2	**Todos los *router*s en el enlace**
FF05::2	**Todos los *router* en el sitio**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

2.4.2.2.5.1Dirección *multicast* de nodo solicitado

Este tipo de direcciones *multicast* de nodo solicitado permiten realizar la asociación entre direcciones MAC y direcciones IPv6. La estructura de esta nueva dirección mantiene parte de la dirección IPv6 que se desea consultar como se observa en la Figura 2-14.

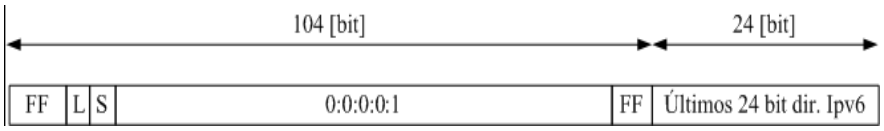

Figura 2-14. Jerarquía de asignación de prefijos de direcciones *unicast* globales
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Cuando un host inicia en IPv6 se une automáticamente al grupo *multicast* indicado por su dirección de nodo solicitado. Su dirección toma solo los últimos 24 bit de la dirección IPv6.

Las nuevas direcciones IPv6 y sus correspondientes direcciones *multicast* de nodo solicitado se pueden observar en la Tabla 2-11.

Tabla 2-11. Direcciones *multicast*de nodo solicitado.

Dirección IPv6	Dirección *multicast* de nodo solicitado
2800:270:bcd0:3::1	**ff02::1:ff00:1**
2800:270::1230:1000:a34:9e9a	**ff02::1:ff34:9e9a**
2800:270::34de:2000:a34:9e9a	**ff02::1:ff34:9e9a**
fc00:0:0:1::aaaa:a1	**ff02::1::ffaa:a1**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Un host al enviar un paquete a un vecino presente en el mismo enlace y del que no conoce su dirección física, envía un mensaje con la dirección IPv6 a consultar al grupo *multicast* de nodo solicitado y todos los nodos que estén en dicho grupo *multicast* reciben el mensaje, respondiendo sólo el host que tiene la dirección IPv6 requerida.

2.4.2.2.6 *Anycast*

Las direcciones *anycast* identifican a un grupo de interfaces. Al enviar un paquete a una dirección *anycast* estos son reenviados por la infraestructura de enrutamiento hacia la interfaz más cercana al origen del paquete.

La dirección *anycast*, se configurará de acuerdo a cada *router* al momento de crear una ruta directa hacia dicha dirección (/128). La idea es que cada *router* posea en su tabla de enrutamiento varias entradas hacia la misma dirección, con sus métricas asociadas y al fallar la ruta más corta, se escoge automáticamente la siguiente. El uso de *anycast* permite principalmente implementar balanceo de carga y tolerancia a fallas.

2.4.2.3 Notación para las direcciones IPv6

El direccionamiento IPv6 tiene las siguientes características para su notación:

- Las direcciones IPv6 son de 128 bits de longitud, representadas en ocho grupos de cuatro dígitos hexadecimales separados por 2 puntos (:)

2001:0cbb:75a3:08d3:1752:4aee:0455:5237

- Se puede cambiar un grupo de cuatro dígitos 0000 por ::

2001:0cbb:75a3:0000:1752:4aee:0455:5237

↓

2001:0cbb:75a3::1752:4aee:0455:5237

- Si más de dos grupos consecutivos son 0L, también se puede cambiar por (::), pero si en la dirección existen más de una serie de grupos 0L consecutivos el cambio sólo se permite en uno de ellos.

2001:0cbb:0000:0000:0000:0000:0455:5237

2001:0cbb:0000:0000:0000::0455:5237

2001:0cbb:0:0:0:0:0455:5237

2001:0cbb:0::0:0455:5237

2001:0cbb::0455:5237

Una dirección no válida es:

2001::0cbb::5237(no válida)

No se sabe cuántos grupos de 0L hay en cada uno

Los ceros iníciales en un grupo se pueden omitir:

2001:0cbb::0455:5237

↓

2001:cbb::0455:5237

- Si la dirección; es una dirección IPv4 que coexiste con IPv6, los últimos 32 bits se representan en decimal:

::ffff:192.168.89.9(decimal)

↘ ↓

::ffff:c0a8:5909(Hexadecimal)

Se pueden tener dos formatos:

::ffff:1.2.3.4(dirección IPv4 mapeada)

::1.2.3.4(dirección IPv4 compatible).

- Las direcciones IPv4 pueden ser transformadas al formato IPv6.

IPv4 192.188.51.3 →C0BC3303en hexadecimal,

0000:0000:0000:0000:0000:0000:C0BC:3303

2.4.2.4 Identificación de los tipos de direcciones

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los primeros bits de cada dirección.

Tabla 2-12. Tipos de Direcciones IPv6

Identificación de los tipos de IPv6	Detalle
::0:0:0:0:0:0:0:0	La dirección con todo cero se utiliza para indicar la ausencia de dirección, y no se asigna ningún host.
::1	Dirección de *loopback* como la 127.0.0.1 en IPv4
::1.2.3.4	La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6.
::ffff:0:0	La dirección IPv4 mapeada se usa como mecanismo de transición en terminales duales.
fe80::	El prefijo de enlace local (link -local) específica que la dirección sólo es válida en el enlace físico local.
fec0::	El prefijo de emplazamiento local
ff00::	El prefijo de *multicast*. Se usa para las direcciones *multicast*.

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

2.5 PAQUETES IPV6

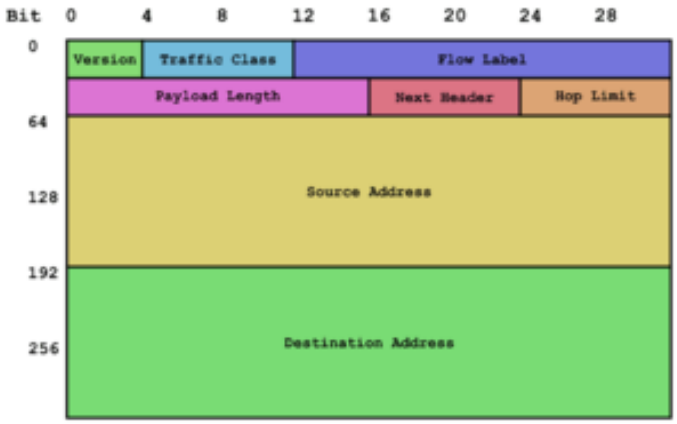

Figura 2-15. Paquete IPv6
Fuente: http://rinkunosekai.blogspot.es/1200676440
Elaborado por: El Autor

Un paquete en IPv6 está compuesto principalmente de dos partes: la cabecera y los datos.

Los primeros 40 bytes (320 bits) son la cabecera del paquete y contiene las direcciones de origen y destino (128 bits cada una), la versión del protocolo IP (4 bits), la clase de tráfico (8 bits, Prioridad del Paquete), la etiqueta de flujo (20 bits, manejo de la Calidad de Servicio), la longitud del campo de datos (16 bits), la cabecera siguiente (8 bits), y el límite de saltos (8 bits, Tiempo de Vida). Después viene el campo de datos, con los datos que transporta el paquete, que puede llegar hasta 64K de tamaño en el modo normal, o más con la opción "*jumbo payload*".

Hay dos versiones de IPv6 levemente diferentes. La ahora obsoleta versión inicial, descrita en el RFC 1883, difiere de la actual versión propuesta de estándar, descrita en el RFC 2460, en dos campos: hay 4 bits que han sido reasignados desde "etiqueta de flujo" (*flowlabel*) a "clase de tráfico" (*trafficclass*).El resto de diferencias son menores.

En IPv6 la fragmentación se realiza sólo en el nodo origen del paquete, al contrario que en IPv4 en donde los *router*s pueden fragmentar un paquete. En IPv6, las opciones también desaparecen de la cabecera estándar y son especificadas por el campo "Cabecera Siguiente" (*NextHeader*), similar en funcionalidad en IPv4 al campo Protocolo. Un ejemplo: en IPv4 uno añadiría la opción "ruta fijada desde origen" (*StrictSource and Record Routing*) a la cabecera IPv4 si quiere forzar una cierta ruta para el paquete, pero en IPv6 uno modificaría el campo "Cabecera Siguiente" indicando que viene una cabecera de encaminamiento. La cabecera de encaminamiento podrá entonces especificar la información adicional de encaminamiento para el paquete.

Este procedimiento es análogo al de AH y ESP en *IPsec* para IPv4 (que aplica a IPv6 de igual modo, por supuesto).

2.5.1 Cabeceras de extensión de IPv6

El uso de un formato flexible de cabeceras de extensión opcionales es una idea innovadora que permite ir añadiendo funcionalidades de forma paulatina. Este diseño aporta gran eficacia y flexibilidad ya que se pueden definir en cualquier momento a medida que se vayan necesitando entre la cabecera fija y la carga útil.

Hasta el momento, existen ocho (8) tipos de cabeceras de extensión, donde la cabecera fija y las de extensiones opcionales incluyen el campo de cabecera siguiente que identifica el tipo de cabeceras de extensión que viene a continuación o el identificador del protocolo de nivel superior. Luego las cabeceras de extensión se van encadenando utilizando el campo de cabecera siguiente que aparece tanto en la cabecera fija como en cada una de las citadas cabeceras de extensión.

Como resultado de la secuencia anterior, dichas cabeceras de extensión se tienen que procesar en el mismo orden en el que aparecen en el datagrama.

La cabecera principal, tiene al contrario que la cabecera de la versión IPv4 un tamaño fijo de 40 octetos.

Todas o parte de estas cabeceras de extensión tienen que ubicarse en el datagrama en el orden especificado:

1. Cabecera de opciones de salto a salto (Hop-by-Hop): transporta información opcional, contiene los datos que deben ser examinados por

cada nodo (cualquier sistema con IPv6) a través de la ruta de envío de un paquete. Su código es 0.

2. Cabecera de encaminamiento (*Routing*): se utiliza para que un origen IPv6 indique uno o más nodos intermedios que se han de visitar en el camino del paquete hacia el destino. El código que utiliza es 43.
3. Encaminamiento desde la fuente.
4. Cabecera de fragmentación (*Fragment*): hace posible que el origen envíe un paquete más grande de lo que cabría en la MTU (Unidad Máxima de Transferencia)de la ruta. Hay que tener en cuenta que al contrario que en IPv4, en IPv6 la fragmentación de un paquete solo se puede realizar en los nodos de origen. El código empleado en esta cabecera es 44.
5. Cabecera de autenticación (*Authentication Header*): nos sirve para proveer servicios de integridad de datos, autenticación del origen de los datos, *anti replay* para IP. El código de esta cabecera es 51.
6. Cabecera de encapsulado de seguridad de la carga útil (*Encapsulating* Security *Payload*): permiten proveer servicios de integridad de datos. El código al que hace referencia esta cabecera es el 50.
7. Cabecera de opciones para el destino (*DestinationOptions*): se usa para llevar información opcional que necesita ser examinada solamente por los nodos destino del paquete. Esta cabecera utiliza el código 60.
8. No *NextHeader*: Indica que no hay más cabeceras Utiliza el código 59.

Cada cabecera de extensión debe aparecer como mucho una sola vez, salvo la cabecera de opción destino, que puede aparecer como mucho dos veces, una antes de la cabecera encaminamiento y otra antes de la cabecera de la capa superior.

2.6 PROTOCOLOS DE ENRUTAMIENTO Y CONTROL IPV6

El uso de IPv6 no implica cambios significativos en la forma en que operan los protocolos de enrutamiento en las redes IP. Sin embargo, para aprovechar las nuevas características de IPv6, se han desarrollado nuevas versiones o complementos a los protocolos de enrutamiento más utilizados. En la Tabla 2-13 se presentan las nuevas versiones desarrolladas para IPv6.

Tabla2-13. Protocolos de enrutamiento en IPv6

Protocolo enrutamiento	Versión IPv6
RIP	RIPng
EIGRP	EIGRP para IPv6
OSPF	OSPFv3
IS-IS	*Integrated* IS-IS
BGP	BGP-MP
EIGRP	EIGRP forIPv6

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

2.6.1 ICMPv6

El protocolo de mensajes de control de Internet (ICMP) es utilizado para enviar información de configuración y reportes de error entre los nodos de una red. Para IPv6, se ha desarrollado una nueva versión del protocolo, denominada ICMPv6 [10]. A diferencia de ICMP para IPv4, el cual no es esencial para las comunicaciones en redes IPv4, ICMPv6 posee características imprescindibles para la configuración y comunicación en redes IPv6. El protocolo ICMPv6 comprende una serie de mensajes, cada uno identificado con un código. Dichos mensajes permiten llevar a cabo diversos procesos en IPv6 tales como: descubrimiento del máximo valor MTU en un camino, manejo de grupos *multicast*, detección de destinos inalcanzables y el protocolo de descubrimiento de vecinos.

2.6.2 Protocolo de descubrimiento de vecinos

El protocolo de descubrimiento de vecinos ("*Neighbor Discovery Protocol",* NDP) es un protocolo necesario para el correcto funcionamiento de las redes IPv6. Es el encargado de descubrir otros nodos en el enlace, realizar la resolución de direccionesIPv6 y direcciones MAC, encontrar los "*routers*" disponibles y mantener información actualizada sobre el estado de los caminos hacia otros nodos.

Este protocolo realiza funciones para IPv6 similares a las realizadas por ARP en IPv4. Para el intercambio de información, utiliza mensajes ICMPv6. En la Tabla 2-14 se presentan las funciones que realiza, junto al equivalente en IPv4.

Tabla 2-14. Características protocolo descubrimiento de vecinos.

Característica de NDP	Descripción	Equivalente IPv4
Descubrimiento de "*routers*"	Permite a los dispositivos detectar a los "*routers*" presentes en el enlace.	ICMP *RouterDiscovery*
Descubrimiento de prefijo	Permite a los nodos conocer el prefijo utilizado en el enlace.	No disponible
Descubrimiento de parámetros	Permite a los nodos auto configurar parámetros como MTU o número máximo de saltos.	PMTU *Discovery*
Autoconfiguración de direcciones	Permite a los dispositivos auto configurar su propia dirección.	No disponible
Resolución de direcciones	Permite a los nodos determinar las direcciones capa 2 de los dispositivos presentes en el enlace.	ARP
Determinación próximo salto	Permite a los nodos determinar el próximo salto para un destino dado.	Tabla ARP y/o tabla de enrutamiento en los dispositivos.
Detección de vecinos inalcanzables(NUD)	Detecta si se puede alcanzar un determinado nodo.	"*Dead* Gateway *Detection*"
Detección de direcciones duplicadas (DAD)	Permite a los nodos determinar si una dirección está en uso.	ARP con origen=0
Redirección	Permite a los "routers" informar a los nodos de un mejor próximo salto para una dirección en particular.	

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

2.6.3 Fragmentación

La fragmentación en IPv6 es manejada únicamente por los nodos finales de una conexión. Los nodos intermedios rechazan todos los paquetes que tengan un tamaño superior a su máxima unidad de transporte (MTU). El MTU mínimo para IPv6 es de 1280 [byte] y el recomendado es de 1500 [byte], superiores a los tamaños establecidos para IPv4 (68 y 576 [byte] respectivamente). Dado que los nodos intermedios no realizan fragmentación, se utiliza el proceso de descubrimiento de la MTU del camino para encontrar la máxima MTU que puede atravesar el camino entre dos nodos. Este proceso utiliza mensajes ICMPv6 y genera una tabla con los valores máximos de MTU para cada destino.

Si un paquete supera el tamaño de la máxima MTU en un camino dado, el nodo origen debe realizar la fragmentación. El proceso de fragmentación es similar del de IPv4, con la diferencia de que en vez de utilizar el campo “fragmentación” de la cabecera IPv4, se utiliza una cabecera adicional para indicar que el contenido del paquete es un fragmento.

2.7 IPV6 Y EL SISTEMA DE NOMBRES DE DOMINIO

Las direcciones IPv6 se representan en el Sistema de Nombres de Dominio (DNS) mediante registros *AAAA* (también llamados registros de *quad-A*, por tener una longitud cuatro veces la de los registros A para IPv4)

El concepto de AAAA fue una de las dos propuestas al tiempo que se estaba diseñando la arquitectura IPv6. La otra propuesta utilizaba registros *A6* y otras

innovaciones como las etiquetas de cadena de bits (*bit-stringlabels*) y los registros *DNAME*.

Mientras que la idea de AAAA es una simple generalización del DNS IPv4, la idea de A6 fue una revisión y puesta a punto del DNS para ser más genérico, y de ahí su complejidad.

La RFC 3363 recomienda utilizar registros AAAA hasta tanto se pruebe y estudie exhaustivamente el uso de registros A6. La RFC 3364 realiza una comparación de las ventajas y desventajas de cada tipo de registro.

2.8 DESPLIEGUE DE IPV6

El 20 de julio de 2004 la ICANN anunció que los servidores raíz de DNS de Internet habían sido modificados para soportar ambos protocolos, IPv4 e IPv6.

2.8.1 Desventajas

- La necesidad de extender un soporte permanente para IPv6 a través de todo Internet y de los dispositivos conectados a ella.
- Para estar enlazada al universo IPv6 durante la fase de transición, todavía se necesita una dirección IPv4 o algún tipo de NAT (compartición de direcciones IP) en los *router*s pasarela (IPv6<-->IPv4) que añaden complejidad y que significa que el gran espacio de direcciones prometido por la especificación no podrá ser inmediatamente usado.
- Problemas restantes de arquitectura, como la falta de acuerdo para un soporte adecuado de IPv6*multihoming*.
- Las direcciones IPv6 son mucho más largas que las direcciones IPv4 y, por lo tanto, más difíciles de memorizar.

2.8.2 Ventajas

- Convivencia con IPv4, que hará posible una migración suave.
- Gran cantidad de direcciones, que hará virtualmente imposible que queden agotadas. Se estima que si se repartiesen en toda la superficie de la Tierra habría $6{,}67 \times 10^{23}$ IP por m^2.
- Direcciones *unicast, multicast y anycast*.
- Formato de cabecera más flexible que en IPv4 para agilizar el encaminamiento.
- Nueva etiqueta de flujo para identificar paquetes de un mismo flujo.
- No se usa ninguna comprobación de integridad (*checksum*).
- La fragmentación se realiza en el nodo origen y el reensamblado se realiza en los nodos finales, y no en los *router*s como en IPv4.
- Nuevas características de seguridad. *IPsec* formará parte del estándar.
- Nueva versión de ICMP, que incluye a MLD, el equivalente del IGMP de IPv4.
- Auto-configuración de los nodos finales, que permite a un equipo aprender automáticamente una dirección IPv6 al conectarse a la red.
- Movilidad incluida en el estándar, que permitirá cambiar de red sin perder la conectividad.

2.8.3 Mecanismos de transición a IPv6

Ante el agotamiento de las direcciones IPv4, el cambio a IPv6 ya ha comenzado. Se espera que convivan ambos protocolos durante 20 años y que la implantación de IPv6 sea paulatina. Existe una serie de mecanismos que permitirán la

convivencia y la migración progresiva tanto de las redes como de los equipos de usuario.

En general, los mecanismos de transición pueden clasificarse en tres grupos:

- Pila dual
- Túneles
- Traducción

La pila dual hace referencia a una *solución de nivel IP con pila dual* (RFC 2893), que implementa las pilas de ambos protocolos, IPv4 e IPv6, en cada nodo de la red. Cada nodo de pila dual en la red tendrá dos direcciones de red, una IPv4 y otra IPv6.

- **A favor**: Fácil de desplegar y extensamente soportado.
- **En contra**: La topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento. Cada nodo en la red necesita tener actualizadas las dos pilas.

Los túneles permiten conectarse a redes IPv6 "saltando" sobre redes IPv4. Estos túneles trabajan encapsulando los paquetes IPv6 en paquetes IPv4 teniendo como siguiente capa IP el protocolo número 41, y de ahí el nombre *proto-41*. De esta manera, se pueden enviar paquetes IPv6 sobre una infraestructura IPv4. Hay muchas tecnologías de túneles disponibles.

La traducción es necesaria cuando un nodo que sólo soporta IPv4 intenta comunicar con un nodo que sólo soporta IPv6. Los mecanismos de traducción se pueden dividir en dos grupos basados en si la información de estado está guardada:

- **Con estado**: NAT-PTRFC 2766, TCP-UDP *Relay*RFC 3142, *Socks-based Gateway*RFC 3089
- **Sin estado**: Bump-in-the-Stack, Bump-in-the-APIRFC 276

Actualmente el protocolo IPv6 está soportado en la mayoría de los sistemas operativos modernos, en algunos casos como una opción de instalación.

Linux, Solaris, Mac OS, *NetBSD, OpenBSD, FreeBSD,* Windows (2000, XP y Vista de forma nativa) y Symbian (dispositivos móviles) son sólo algunos de los sistemas operativos que pueden funcionar con IPv6.

2.8.4 Anuncios importantes sobre IPv6

- En 2003, Nihon Keizai Shimbun informa que Japón, China y Corea del Sur tomaron la determinación de convertirse en una de las naciones líderes en la tecnología de Internet, que conjuntamente han dado forma parcialmente al desarrollo de IPv6, y que lo adoptaron completamente a partir de 2005.

- ICANN anunció el 20 de julio de 2004 que los registros AAAA de IPv6 de código de país para Japón (.jp) y Corea (.kr) ya son visibles en los servidores raíz de DNS. El registro IPv6 para Francia (.fr) fue añadido poco después.

- El 4 de febrero de 2008 se añade a los servidores raíz de la red (Master Address books) un pequeño número de registros que están escritos en IP versión 6 (IPv6). Esto significa que por primera vez las máquinas que utilicen IPv6 pueden encontrarse una a la otra sin la participación de toda la tecnología IPv4.

- Desde el 2006 muchos sistemas operativos han estado trabajando en IPv6 paralelamente con IPv4, sistemas como GNU/Linux, Mac, Unix y Windows. En 2008 las redes empresariales que cuenten con Servidores Windows Server 2008 y a Windows Vista como "cliente" ya utilizan el protocolo IPv6 para comunicarse entre sí prescindiendo de la tecnologíaIPv4, que solo se utiliza para comunicaciones a Internet.

CAPÍTULO III

SITUACIÓN ACTUAL DE LA RED DE LA UTE

En este capítulo se analizará la situación actual de la red de la Universidad, para identificar los dispositivos compatibles que intervendrán en la implementación deIPv6.

Se analiza la red de la Universidad tomando en cuenta los siguientes puntos:

- La infraestructura Física y Lógica que maneja actualmente la red de la Universidad.
- Detalle de equipos y dispositivos que forman parte de la red.
- Servidores de Correo, DNS, Web y DHCP.
- Servicios en los que se Implementaría IPv6 en Doble –Pila.
- Análisis de factibilidad.

3 INFRAESTRUCTURA ACTUAL DE LOS CAMPUS Y CENTRO DE APOYO DE LA UTE.

La Universidad Tecnológica Equinoccial está conformada por varios Campus y Centros de Apoyo localizados en las diferentes provincias del Ecuador, en la tabla 3.1 se expone una lista de acuerdo a la cuidad que se encuentran ubicadas.

En la actualidad se cuenta con tres Campus y 14Centros de Apoyo a nivel Nacional y cada una de ellas cuenta con sus propias redes internas locales (LAN).

Tabla 3-1. Campus y Centros de Apoyo de la UTE

Tipo	Ubicación
Campus	Quito – (Rumipamba y Occidental)
Campus	Santo Domingo
Campus	Salinas
Centro de Apoyo	Guayaquil
Centro de Apoyo	Manta
Centro de Apoyo	Loja
Centro de Apoyo	Ibarra
Centro de Apoyo	Ambato
Centro de Apoyo	Riobamba
Centro de Apoyo	Cuenca
Centro de Apoyo	Machala
Centro de Apoyo	Bahía de Caráquez
Centro de Apoyo	Azogues
Centro de Apoyo	Tulcán
Centro de Apoyo	Lago Agrio
Centro de Apoyo	Chone
Centro de Apoyo	Puyo

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Estos sitios se encuentran interconectados a través de enlaces de datos con topología estrella cuyo punto central es Quito.

Tomando en cuenta el tamaño de la infraestructura de red, se analizará por separado los campus Quito, Santo Domingo, Salinas y los centros de apoyo por tener una infraestructura muy pequeña y similar se los agrupará en un solo análisis para su compatibilidad con IPv6.

3.1 INFRAESTRUCTURA DE LAS REDES INTERNAS DE LA UTE (INTRANETS)

3.1.1 Red interna Campus Quito (Rumipamba - Occidental)

Estos dos sitios actualmente se encuentran interconectados por enlaces privados de fibra óptica como se puede observar en la Figura 3.1, las velocidades de trasmisión son de 3 Gbps en *etherchannel*, se podría considerar que estos dos sitios forman una red de área metropolitana (MAN), aunque su configuración de red lógica es de una red de área local (LAN).

Figura 3-1. Enlace de fibra óptica propio entre Rumipamba y Occidental
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

3.1.2 Interconexión de los equipos de *Core* de los sitios Occidental y Rumipamba

Para un mejor manejo del tráfico de datos se tiene instalado los *switches* de *Core* en cada uno de los sitios Rumipamba y Occidental, el ruteo interno y el ruteo hacia Internet está centralizado en la Occidental en donde se concentra el corazón de la infraestructura.

En la Figura 3.2 se puede observar esta conexión entre los dispositivos.

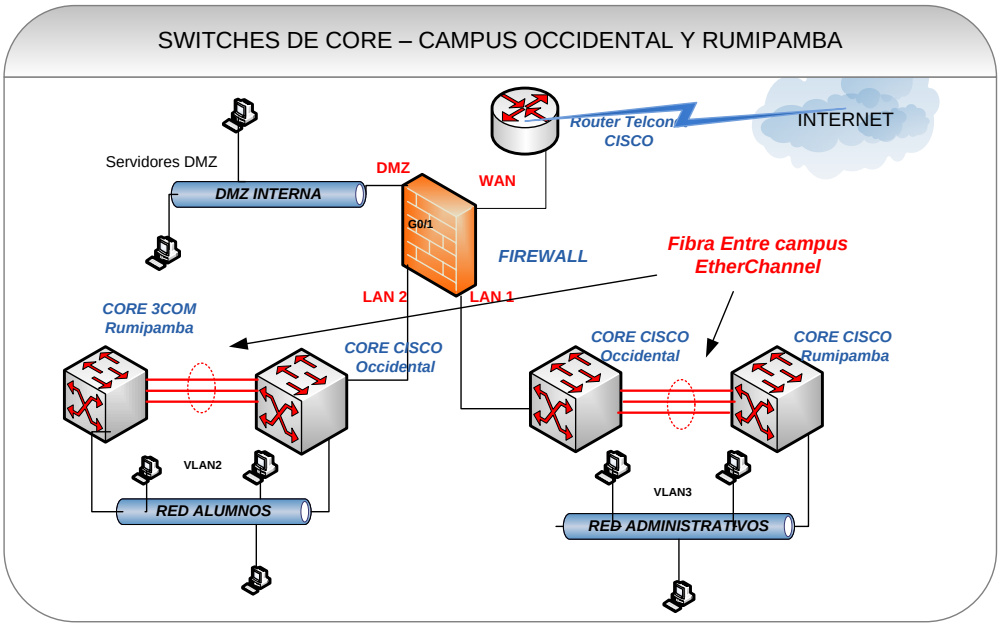

Figura 3-2. Conexión de los *switches* de *Core* entre los campus y hacia Internet
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Las redes internas de estos sitios Occidental y Rumipamba están implementadas y configuradas físicamente separadas en dos redes independientes que son:

- Red Administrativa
- Red Alumnos

3.1.2.1 Dispositivos que intervendrán en la migración a IPv6 en la Red Administrativa

Para indicar e identificar los equipos y dispositivos que hay en estos campus, se los clasificará de acuerdo a la división antes mencionada en la red Interna administrativa y alumnos.

1. Equipos de Interconectividad. (*Switches*)

Tabla3-2. *Switches* del área administrativa sitios Rumipamba y Occidental

SWITCHES RED ADMINISTRATIVA				
Ítem	**MARCA**	**MODELO**	**OBSERVCIONES**	**CANT.**
2	CISCO	WS-C2960-24TT-L	IOS versión 12.2	20
3	CISCO	WS-C2960-24TC-L	IOS versión 12.2	4
4	CISCO	WS-CE500-24TT	IOS versión 12.2	15
5	CISCO	WS-C4503	IOS versión 12.2	2
6	CISCO	C2950-C3H2S-M	IOS versión 12.2	1
7	CISCO	WS-CE500-24LC	IOS versión 12.2	1
8	CISCO	WS-C2960-48TT-L	IOS versión 12.2	13
9	CISCO	WS-C2960-48TC-L	IOS versión 12.2	15
10	3COM	Switch 4400	6.10	1
11	CISCO	WS-C6506-E	IOS versión 12.2	1
			SUBTOTAL	**73**
			TOTAL	**73**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los equipos de *networking* (*switches*) utilizados en la red administrativa son 72*switches CISCO y 1 switch 3COM* como se puede observar en la Tabla 3.2. Todas las versiones de dispositivos que se tienen soportan IPv6.

2. Equipos de Uso en el puesto de trabajo

Aquí se mencionan los equipos y dispositivos que se tienen instalados en los puestos de trabajo de los usuarios que cumplen los roles del personal administrativo.

Tabla3-3. Computadores de la red administrativa

COMPUTADORES EN RED ADMINISTRATIVA						
Item	**DISPOSITIVO**	**CARACTERÍTICAS**	**Win XP**	**Win 7**	**Win 2008**	**TOTAL**
1	Computadores de Escritorio	PIV a Core i7	10	410	20	440
2	Computadores Portátiles	PIV a Core i7	15	6	1	22
3	Equipos MAC		-	-	-	5
SUBTOTAL						**467**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los computadores de la red administrativa están actualizados en sistemas operativos y programas, que permiten el manejo de IPv6 sin ningún problema.

Tabla 3-4. Impresoras de red para uso de Administrativos

IMPRESORAS DE RED ADMINISTRATIVA			
Item	**DISPOSITIVO**	**CARACTERÍTICAS**	**CANT.**
1	Impresoras en Red .	HP 2600, Hp 1320n, 2015n, HP 3600n, HP 3500n	140
SUBTOTAL			**140**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Las impresoras presentan ya en sus sistemas compatibilidad con IPv6.

3. Equipos de uso General

Tabla 3-5. Teléfonos IP Red Administrativos

TELÉFONOS IP EN RED ADMINISTRATIVA				
Ítem	**DIPOSITIVO**	**MODELO**	**MARCA**	**CANT.**
1	Teléfono IP de teclado	ITR 8D	NEC	318
2	Teléfono IP de teclado	ITR 4D	NEC	2
TOTAL				**320**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Lo teléfonos que se mencionan en la tabla 3.5 no son compatibles con IPv6.

Tabla 3-6. Cámara IP Red Administrativos

CÀMARAS IP EN RED ADMINISTRATIVA				
Ítem	**DIPOSITIVO**	**MODELO**	**MARCA**	**CANT.**
1	Cámaras IP	AXIS 211 Network Camera version 4.30a	AXIS	328
TOTAL				**328**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Las cámaras Axis son compatibles con IPv6.

Tabla3-7. Relojes Biométricos IP Red Administrativos

RELOJES BIOMÉTRICOS IP EN RED ADMINISTRATIVA				
Ítem	**DIPOSITIVO**	**MODELO**	**MARCA**	**CANT.**
1	Reloj Biométrico	*HandPunch* 4000	*HandPunch*	2
2	Reloj Huella			6
TOTAL				**8**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los relojes biométricos de mano y los relojes para la huella del dedo no son compatibles con IPv6.

3.1.2.2 Dispositivos que intervendrán en la migración a IPv6 en la Red Alumnos

1. Equipo de Interconectividad. (*Switches*)

Tabla 3-8. *Switches* de Red de Alumnos

*SWITCHES*RED ALUMNOS				
Ítem	**MARCA**	**MODELO**	**OBSERVCIONES**	**CANT.**
2	CISCO	WS-C2960-24TT-L	IOS version 12.2	15
3	CISCO	WS-C2960-24TC-L	IOS version 12.2	11
4	CISCO	WS-CE500-24TT	IOS version 12.2	3
5	CISCO	WS-C4503	IOS version 12.2	1
6	CISCO	C2950-C3H2S-M	IOS version 12.2	2
7	CISCO	WS-CE500-24LC	IOS version 12.2	1
8	CISCO	WS-C2960-48TT-L	IOS version 12.2	15
9	CISCO	WS-C2960-48TC-L	IOS version 12.2	10
10	3COM	Switch 4400	6.10	7
SUBTOTAL				**65**
TOTAL				**65**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los *Switches* que manejan el tráfico en la red de alumnos, son los mismos modelos que se tiene en la red administrativa, con la diferencia que existen mayor número de equipos marca 3com, que debido a que se quiere manejar un solo modelo de estos equipos de marca Cisco, se los reemplazará en el transcurso de este año.

2. Equipos de Uso en el puesto de trabajo

Los equipos que se listan en la Tabla 3.9 corresponden a los equipos que se tiene instalados en los laboratorios de toda la Universidad y que manejan sistemas operativos y programas con la misma configuración, estandarizados y de versiones actuales.

Tabla 3-9. Computadores de laboratorios en alumnos

COMPUTADORES EN RED ALUMNOS						
Ítem	**DISPOSITIVO**	**CARACTERÍTICAS**	**Win XP**	**Win7**	**Win 2008**	**TOTAL**
1	Computadores de Escritorio	PIV a Core i7	20	846	10	876
SUBTOTAL						**876**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

3. Equipos de Acceso Inalámbricos (*Wireless)*

La Universidad tiene en casi toda su infraestructura el servicio *wireless*, estos se conectan a través de la red de alumnos en donde se manejan ciertas políticas de autentificación, todos estos equipos son compatibles con IPv6 y se listan en la Tabla 3.10.

Tabla 3-10. Equipos *Wireless* AP

EQUIPOS WIRELESS AP ALUMNOS				
Ítem	**MARCA**	**MODELO**	**OBSERVCIONES**	**CANT.**
1	CISCO	AIR-AP1252G-A	12.4(10b)JA1	30
2	CISCO	AIR-BR1310G-A-K9	12.4(10b)JA1	3
3	LINKSYS	WRT300N		5
4	3COM			3
SUBTOTAL				**41**
TOTAL				**41**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

3.1.2.3 Campus Santo Domingo

En el campus Santo Domingo se maneja la siguiente infraestructura de red:

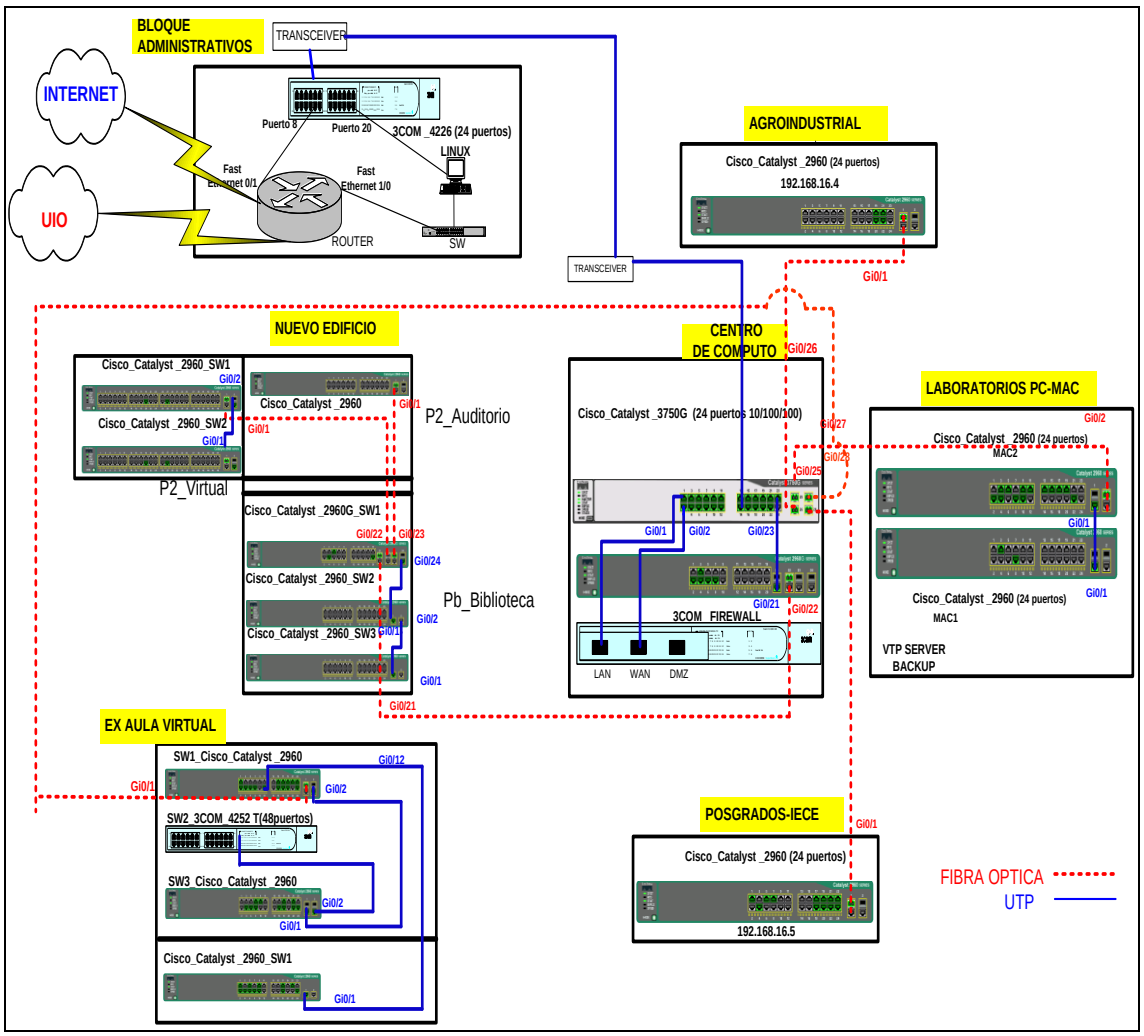

Figura 3-3. Estructura de red Campus Santo Domingo
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los dispositivos que actualmente se disponen en la red del Campus Santo Domingo son de modelos y marcas similares a las que se manejan en Quito, con la diferencia que la red alumnos y administrativa no son físicamente separadas, la separación se la realizó a nivel de *vlans* o redes virtuales.

A continuación se muestra en la Tabla 3.11 un resumen de todos los dispositivos que se tienen instalados de acuerdo a su ubicación.

Tabla 3-11. Dispositivos Campus Santo Domingo

SANTO DOMINGO	Servidores	Computadores	Laptops	Macintosh	Impresoras	Cámaras IP
CENTRO DE COMPUTO	6	48	0	30	3	2
OFICINAS	0	46	3	0	18	0
LABORATORIOS	0	48	0	30	2	0
BODEGA	0	10	0	0	0	0
TOTAL	**6**	**152**	**3**	**60**	**23**	**2**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los sistemas operativos de los servidores y computadores están actualizados con las últimas versiones que son compatibles con IPv6.

Las impresoras y cámaras IP son compatibles con IPv6

Tabla 3-12. *Switches* Campus Santo Domingo

SWITCHES				
Ítem	**MARCA**	**MODELO**	**OBSERVCIONES**	**CANT.**
1	CISCO	WS-C2960-24TT-L	IOS versión 12.2	2
2	CISCO	WS-C2960G-24TC-L	IOS versión 12.2	2
3	CISCO	WS-CE500-24LC	IOS version 12.2	1
4	CISCO	WS-C3750G	IOS version 12.2	1
4	3COM	4400 SE	5.1	1
TOTAL				16

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los *Switches* son los mismos modelos que se tienen en la matriz, por lo tanto son compatibles con IPv6.

Además se tiene instalados equipos de acceso inalámbricos de marca *linksys* que son compatibles con IPv6.

La telefonía es la tradicional y no se la tomará en cuenta para IPv6.

3.1.2.4 Campus Salinas

La red en salinas se encuentra estructurada de la siguiente forma:

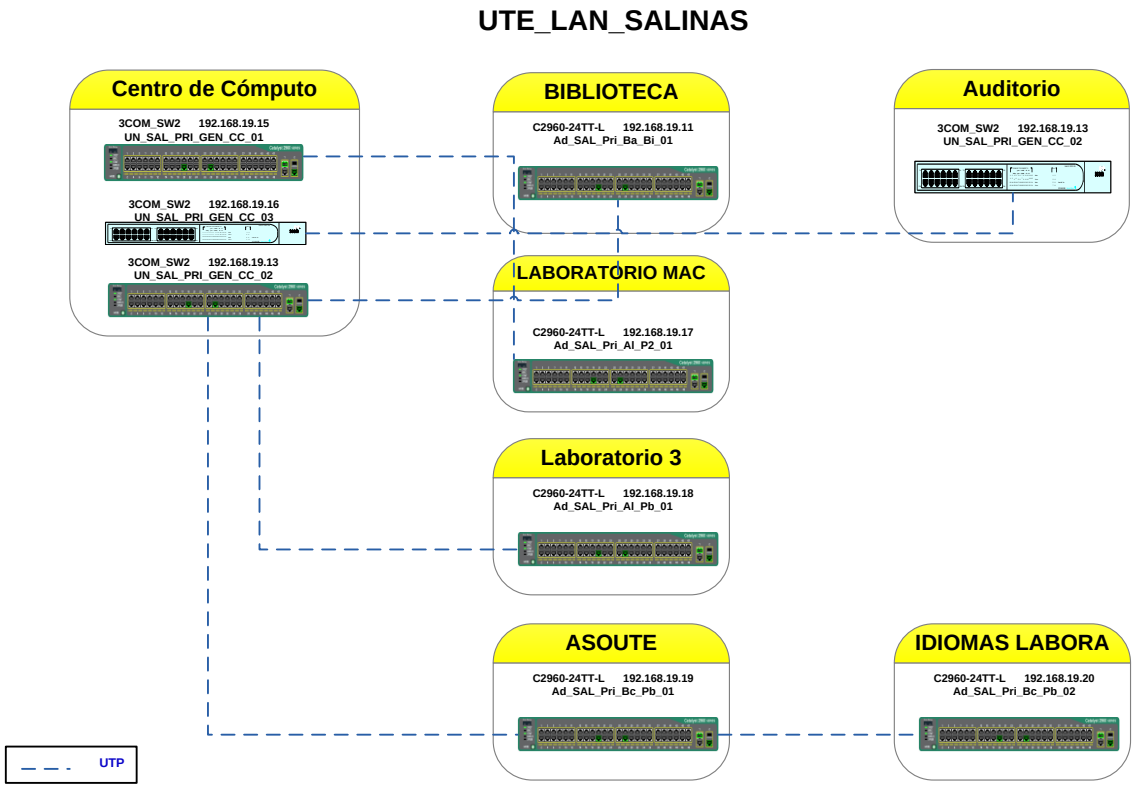

Figura 3-4. Estructura Campus Salinas
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

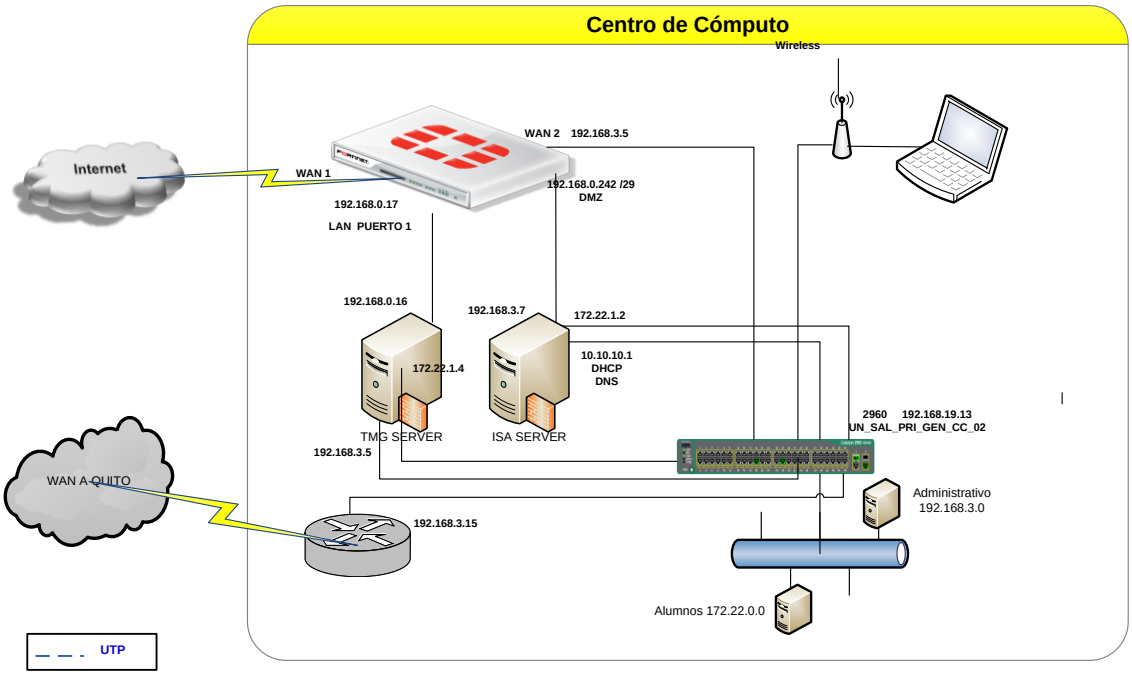

Figura 3-5. Red de Internet - WAN Salinas
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los dispositivos que están conectados a la red de datos son:

Tabla 3-13. Dispositivos Campus Salinas

SALINAS	Servidores	Computadores	Laptops	Macintosh	ApWifi	Impresoras	Cámaras IP
LABORATORIOS	0	31	0	15	1	0	0
CENTRO DE COMPUTO	7	0	1	0	1	0	1
OFICINAS	0	13	2	0	4	8	0
TOTAL	**7**	**44**	**3**	**15**	**6**	**8**	**1**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los sistemas operativos de los servidores y computadores están actualizados con las últimas versiones que son compatibles con IPv6.

Las impresoras de red, Access Point y cámaras IP son compatibles con IPv6.

No se maneja telefonía IP solo la tradicional que no interviene en IPv6.

Tabla 3-14. Switches Campus Salinas

SWITCHES				
Ítem	**MARCA**	**MODELO**	**OBSERVCIONES**	**CANT.**
1	CISCO	WS-C2960-24TT-L	IOS versión 12.2	4
2	CISCO	WS-C2960G-24TC-L	IOS versión 12.2	2
3	CISCO	WS-CE500-24LC	IOS versión 12.2	1
4	3COM	4400 SE	5.1	3
TOTAL				10

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los *Switches* son los mismos modelos que se tienen en la matriz, por lo tanto son compatibles con IPv6.

3.1.2.5 Centro de Apoyo - Guayaquil

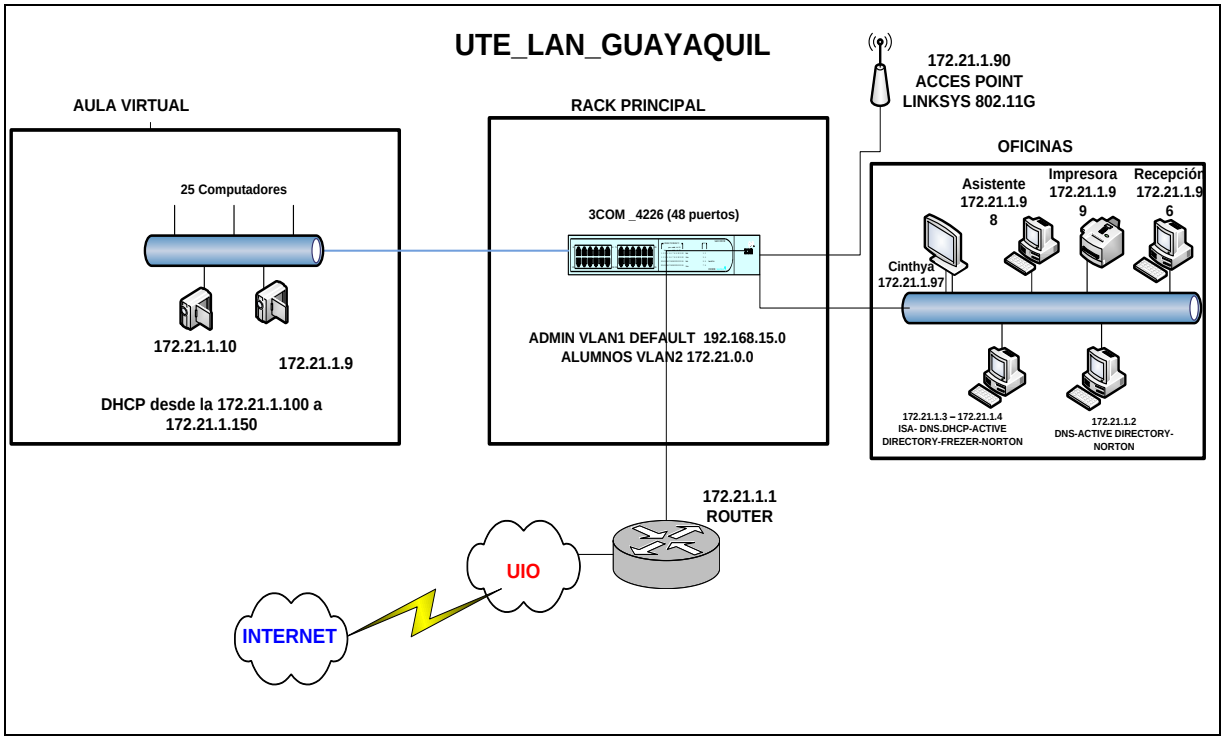

Figura 3-6. Estructura Campus Guayaquil
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los dispositivos que están conectados a la red de datos son:

Tabla 3-15. Dispositivos Campus Guayaquil

GUAYAQUIL	Servidores	Computadores	Laptops	Macintosh	AP wifi	Impresoras de red	Cámaras IP
LABORATORIOS	0	25	0	0	1	0	0
OFICINAS	0	3	0	1	0	2	0
TOTAL	**0**	**28**	**0**	**1**	**1**	**2**	**0**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los sistemas operativos de los servidores y computadores están actualizados con las últimas versiones que son compatibles con IPv6.

Las impresoras de red, Access Point y cámaras IP son compatibles con IPv6.

Tabla 3-16. Switches Campus Salinas

SWITCHES				
Item	**MARCA**	**MODELO**	**OBSERVCIONES**	**CANT.**
1	CISCO	WS-C2960-24TT-L	IOS versión 12.2	1
4	3COM	4400 SE	5.1	1
	TOTAL			2

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los *Switches* son los mismos modelos que se tienen en la matriz, por lo tanto son compatibles con IPv6.

3.1.2.6 Centros de Apoyo

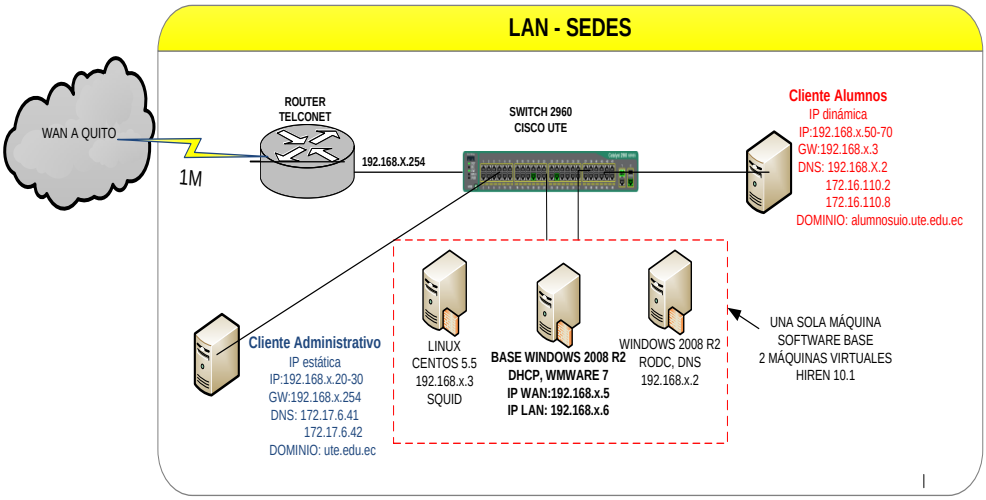

Figura 3-7. Infraestructura de los centros de Apoyo
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

La infraestructura de red lógica de todos los centros de apoyo de la Universidad que está ubicados en las diferentes provincias del País, manejan un esquema idéntico de configuraciones y dispositivos, por eso se mencionó anteriormente que solo se ubicará o expondrá un prototipo que representará a todos los centros de apoyo.

Tabla 3-17. Dispositivos que se encuentran en los centros de apoyo

Centros Apoyo	Servidores	Computadores	Laptops	Macintosh	AP wifi	Impresoras	Cámaras IP
LABORATORIOS	0	10	0	0	1	0	0
OFICINAS	3	1	0	0	0	1	0
TOTAL	**0**	**28**	**0**	**1**	**1**	**1**	**0**

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Tabla 3-18. *Switches* Campus Salinas

SWITCHES				
Ítem	**MARCA**	**MODELO**	**OBSERVACIONES**	**CANT.**
1	CISCO	WS-C2960-24TT-L	IOS versión 12.2	1
	TOTAL			2

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Todos los dispositivos que se tiene instalados en las sedes son compatibles con IPv6, y no se maneja telefonía IP.

3.1.3 WAN UTE

A continuación se detalla un esquema de la infraestructura de la red WAN que une a través de enlaces de datos los campus de Quito con todas las sedes.

La Universidad cuenta con enlaces principales y de *backup* como se puede observar en la Figura 3.8.

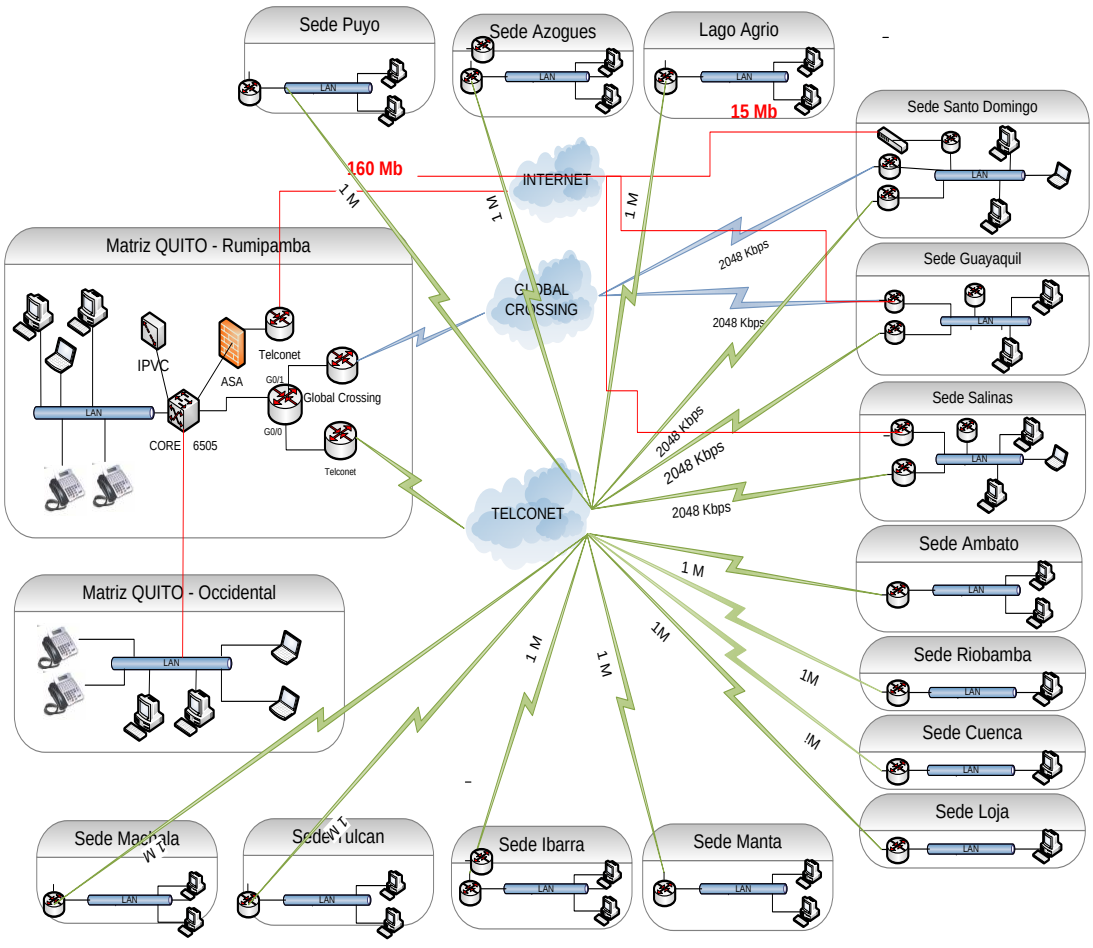

Figura 3-8. Estructura WAN UTE
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los equipos que se manejan para la interconectividad son los siguientes:

Tabla 3-19. *Routers* WAN UTE

ROUTERS				
Ítem	**MARCA**	**MODELO**		**CANT.**
1	CISCO	2821		1
2	CISCO	2610		1
3	CISCO	1721		3
4	CISCO	1841		3
TOTAL				8

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Las principales características que se tiene de este esquema de infraestructura WAN son:

- Enlaces de Datos de 1 y 2 Megabytes hacia todos los Campus, Sedes y Centros de Apoyos, con conexión centralizada y controlada desde las instalaciones de la Av. Mariscal Sucre en Quito.

- Dos enlaces de datos en el Campus Santo Domingo y Centro de Apoyo de Guayaquil para redundancia con diferentes proveedores.

- Enlaces independientes para acceso a Internet desde los campus Santo Domingo, Salinas y Centro de Apoyo de Guayaquil.

- Los equipos de Conectividad *Routers* son propiedad de los proveedores, por lo que se pidió a Telconet que levante en todos sus equipos las configuraciones IPv6para la comunicación entre todas las sedes.

CAPÍTULO IV

DISEÑO E IMPLEMENTACIÓN DE LOS SERVICIOS SOBRE IPv6.

4 RECURSO INFORMÁTICO Y HUMANO

El Recurso Informático que se utilizará para realizar este proyecto es el siguiente:

4.1 RECURSO INFORMÁTICO

Un computador para pruebas con XP, Vista, Windows 2008 y Linux

Disponibilidad de dispositivos para las pruebas como son:

- Cámara IP
- *Wireless* AP
- *Router*
- *Switch*
- Impresoras de Red

4.1.1 Recurso Humano

Tres (3) Ingenieros de Mantenimiento - Redes.

4.1.2 Recursos adicionales

- ❖ Horas extras en cambio fuera de horario
- ❖ Pasajes de ida y regreso de las sedes
- ❖ Alojamiento para los técnicos
- ❖ Alimentación para los técnicos

4.2 DISEÑO IPV6 SOBRE LA REDES INTERNAS DE LA UNIVERSIDAD

En la Figura 4.1 se presenta el diagrama del *backbone*, con la configuración de IPv6 que se ha implementado.

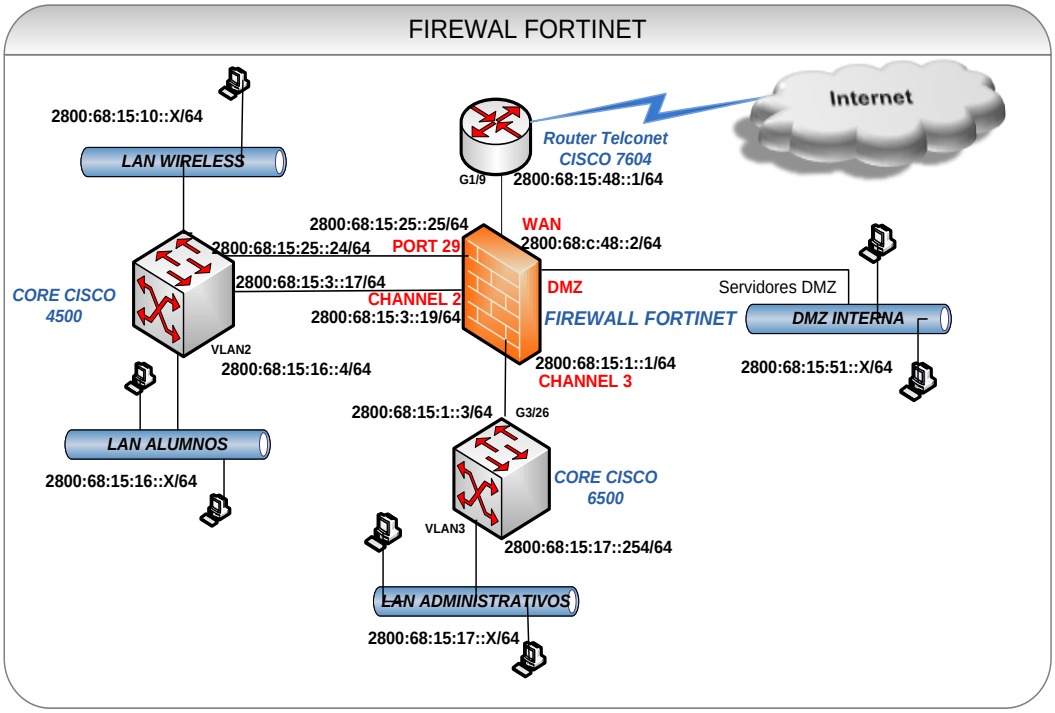

Figura 4-1. Direccionamiento IPv6 de los equipos de conectividad de la red interna
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Este direccionamiento se lo ha realizado, tomando en cuenta el nuevo protocolo IPv6 y manteniendo una estructura similar al direccionamiento IPv4que se tiene actualmente implementado. En la Tabla 4.1 se indica los rangos de las direcciones IPv6 que se han asignado.

Tabla 4-1. Direccionamiento IPv6 de las redes internas

RED	Red IPv6	Gateway	DNS	#host
LAN ADMINISTRATIVA	2800:68:15:17::x/64	2800:68:15:17::254	2800:68:15:17::1	2^{80} hosts
LAN ALUMNOS	2800:68:15:16::x/64	2800:68:15:16::4	2800:68:15:16::8	2^{80} hosts
LAN WIRELESS	2800:68:15:10::x/64	2800:68:15:10::1	2800:68:15:10::2	2^{80} hosts

Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Los primeros tres números hexadecimales 2800:68:15 se mantienen en las redes internas como se puede observar en la Tabla 4.1, estos han sido asignados a la UTE como miembro de CEDIA, que es el organismo representante de las redes académicas en el Ecuador y uno de los proyectos que está impulsando es IPv6.

Para la implementación de IPv6 sobre la red administrativa y la red alumnos, se ha procedido con el detalle específico en cada equipo y dispositivo que forman parte de esta red, tomando en cuenta que la mayoría de servicios y aplicativos están implementados en la red administrativa, debido a que manejan en la mayoría de los casos similares plataformas y equipos.

Para la implementación de la red de alumnos, solo se mencionará las configuraciones que son diferentes y puntuales para que no se repita las mismas.

4.2.1 Implementación de IPv6 sobre la red Administrativa.

En la red administrativa se encuentran la mayoría de servicios de red como:

- Servidor web principal www.ute.edu.ec
- Servidor de Correo
- Servidor de base de datos
- Servidor DNS
- Servidor DHCP
- Servidor de Aplicaciones de escritorio
- Telefonía IP
- Cámaras IP

En esta sección nos enfocaremos en los servicios y equipos que son parte fundamental para la implementación y funcionamiento de IPv6.

4.2.1.1 Instalación de los Sistemas de Nombres de dominio para resolución de IPv6 (DNS)

La configuración se realizó sobre los servidores de Directorio Activo que trabajan conjuntamente como *DNS*, el sistema operativo instalado es *Windows* 2008 server.

Por defecto los sistemas *Windows* 2008 *server*, ya permiten ampliamente soporte IPv6, para lo cual primeramente se debe asignar la dirección IPv6 de acuerdo a la configuración del administrador.

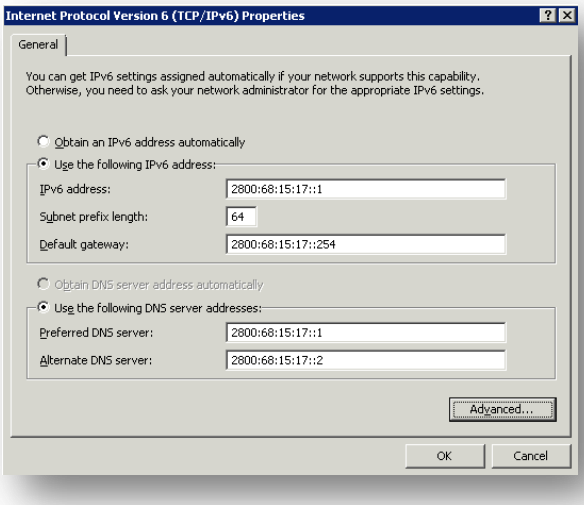

Figura 4-2. Configuración de la dirección IPv6 en la interface de red del servidor
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Luego de asignar estáticamente una dirección IPv6 del bloque 2800:68:15:17 como se observa en la Figura 4.2, se procede a configurar el servicio DNS.

Lo primero que tenemos que crear es la zona reversa como se muestra en la Figura 4.3, ingresando al servicio DNS que se encuentra en herramientas administrativas del servidor.

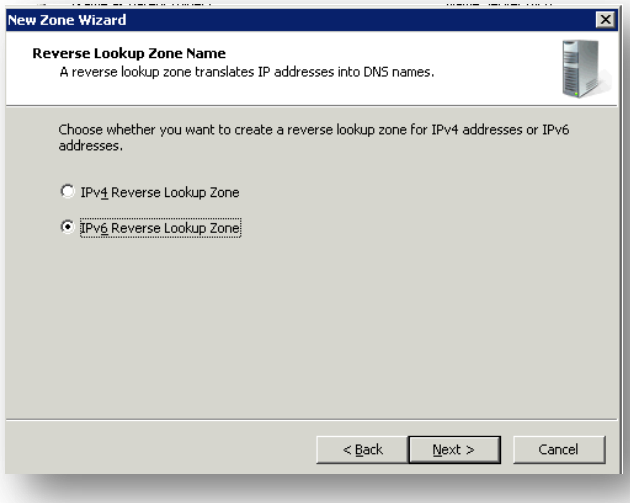

Figura 4-3. Creación de una nueva zona reversa IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Se ingresa el prefijo de la red administrativa como se puede observar en la Figura 4.4.

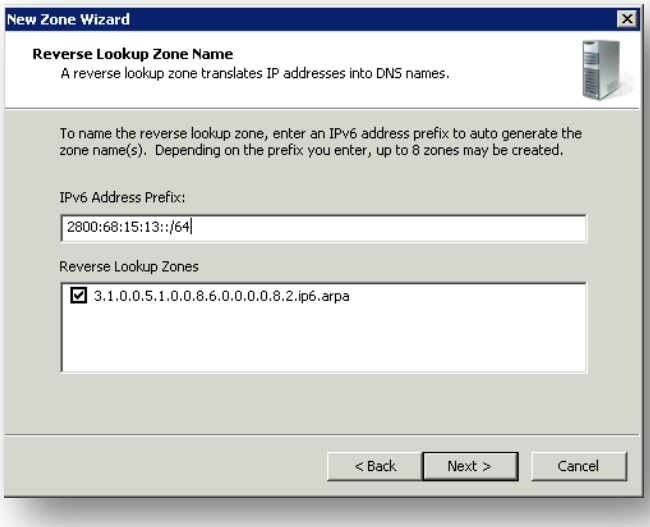

Figura 4-4. Ingreso del Prefijo de la dirección IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Una vez creada la zona reversa, se crean automáticamente los punteros en los equipos que su sistema operativo ya tiene instalado IPv6, en la Figura 4.5 se muestra las zonas creadas y los punteros que se han registrado.

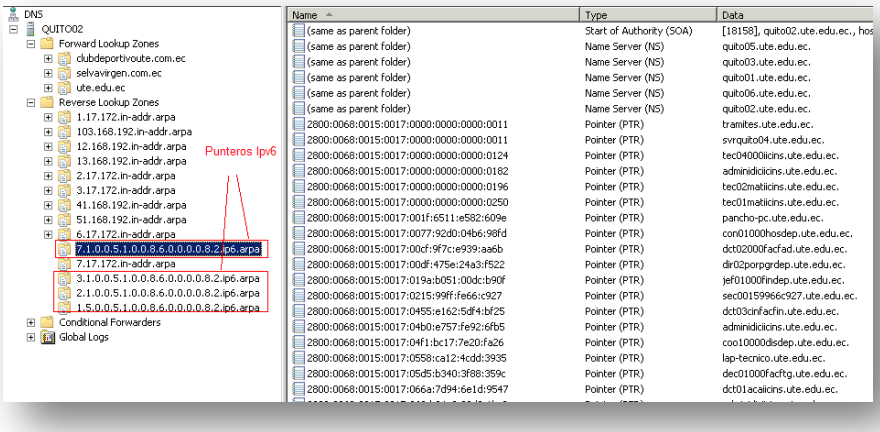

Figura 4-5. Punteros creados en el servidor DNS
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Estas configuraciones se las debe realizar en todos los servidores DNS, tanto en la red administrativa como en la red de alumnos se tiene instalados los DNS con la misma plataforma.

4.2.1.2 Instalación del Protocolo Configuración Dinámica de dispositivos IPv6 (DHCP6)

Otro servicio importante que se ha configurado es el servidor de asignación dinámica de IP (DHCP), Este servicio trabaja idénticamente que en la versión 4 y en *Windows* 2008 server ya tiene soporte y es totalmente compatible. El procedimiento de configuración bajo esta plataforma se describe a continuación.

El primer paso es crear un *scope* o rango en el mismo servicio *dhcp* v4 dentro de herramientas administrativas como se muestra en la Figura 4.6.

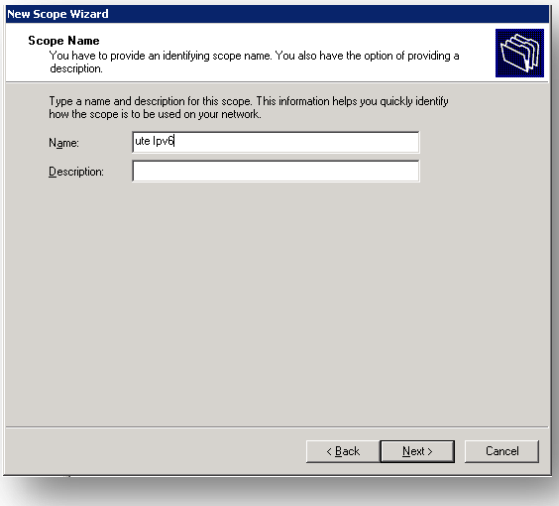

Figura 4-6. Creación de un nuevo ámbito de direcciones IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Ingresamos el prefijo o el rango que deseamos asignar automáticamente como se observa en la Figura 4.7.

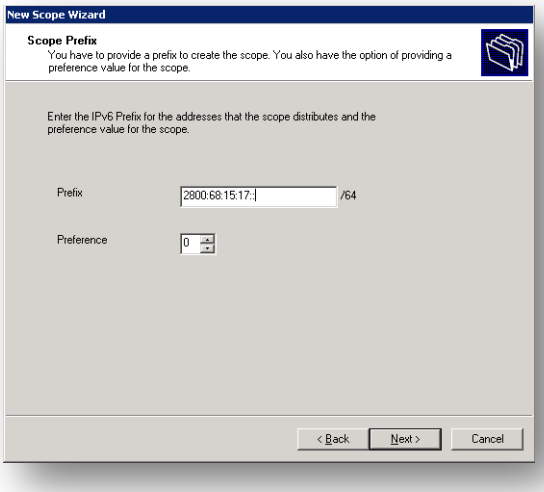

Figura 4-7. Definición del prefijo del ámbito
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la Figura 4.8 podemos observar el rango habilitado para esta red conservando los cuatro (4) primeros números hexadecimales.

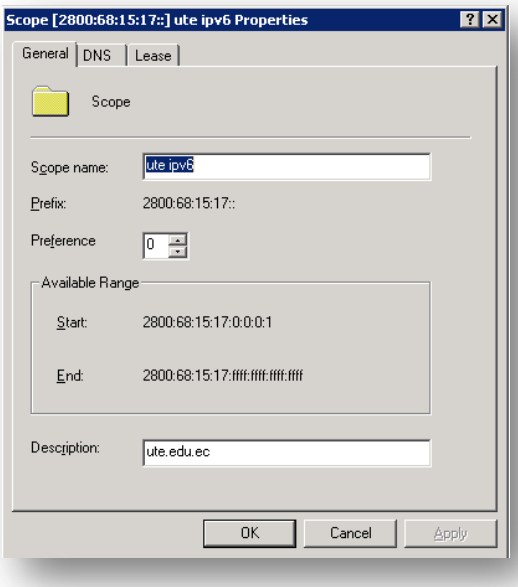

Figura 4-8. Configuración de las propiedades del alcance del ámbito
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la Figura 4.9 podemos verificar que automáticamente el servidor empieza ya a asignar las direcciones IPv6 sin interferir en las direcciones IPv4, coexistiendo las dos versiones sin problemas.

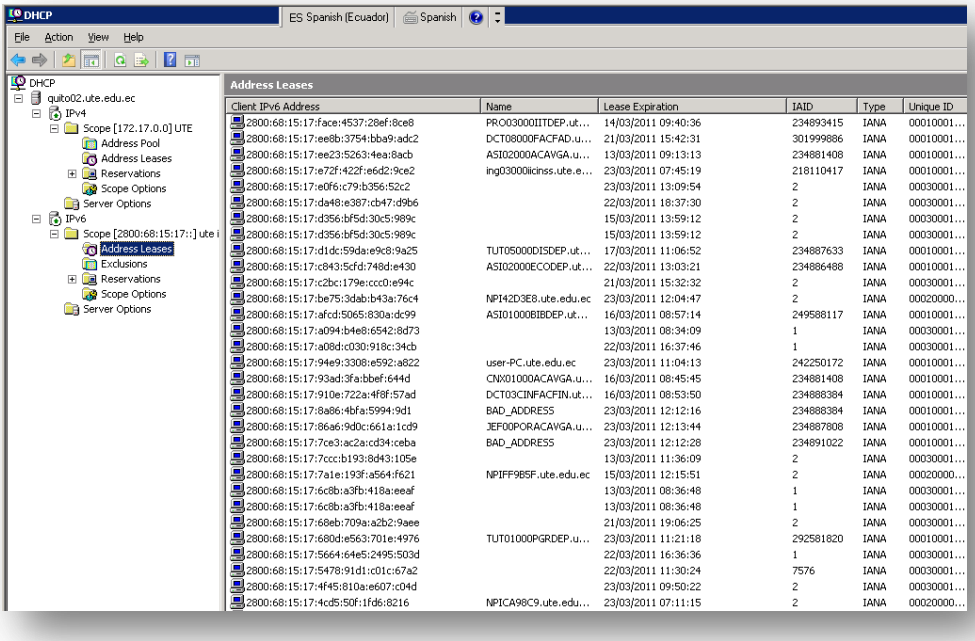

Figura 4-9. DHCP administrativo IPv6 y IPv4
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.2.1.3 Configuración en el servidor de Correo

En la Universidad el servidor de correo que se tiene implementado es el Exchange 2007 bajo el sistema operativo Windows 2008 server, para la configuración de IPv6 se debe aplicar lo siguiente:

- El primer paso es asignar una dirección IPv6 estática de la red administrativa en cada servidor que tenga configurado exchange2007, siendo importante el uso de los DNS correctos, en la Figura 4-10 se observa la dirección configurada en uno de los servidores.

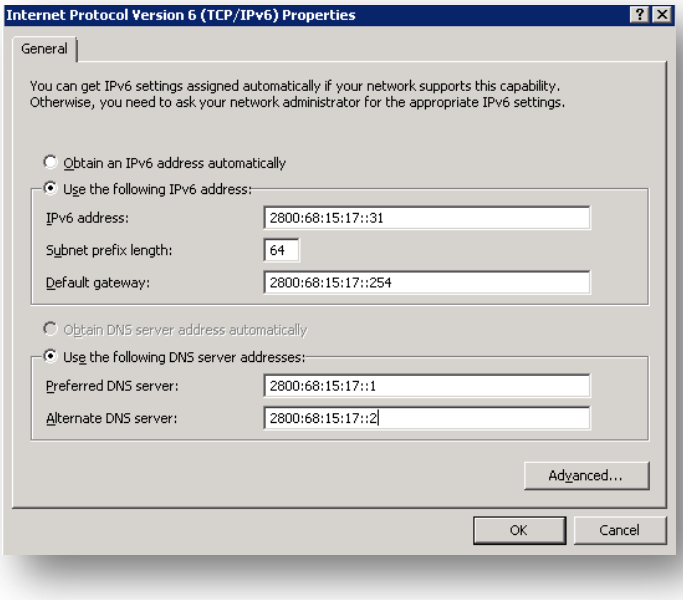

Figura 4-10. Asignación de la dirección IPv6 en el servidor de correo
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

- Se debe agregar en las propiedades del conector de la consola de Exchange 2007, la dirección IPv6 correspondiente al servidor que enruta todo el tráfico de correo hacia el exterior como se puede visualizar en la Figura 4-11.

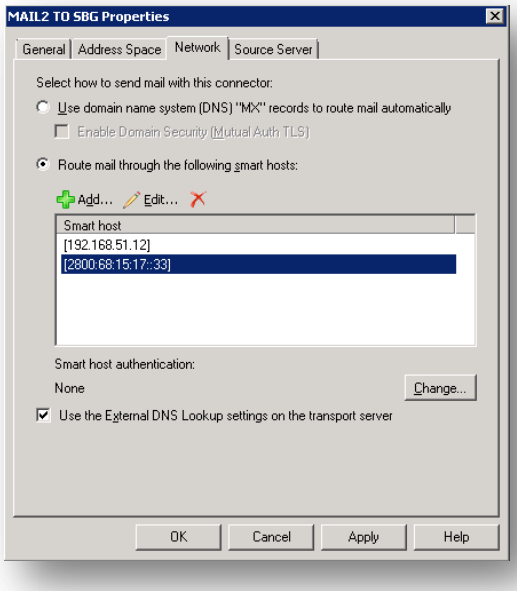

Figura 4-11. Configuración del conector para Exchange 2007
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

- En las propiedades de servidor en la consola de Exchange 2007 se debe agregar tanto los DNS internos y externos que resuelven los nombres sobre IPv6, esta configuración se puede observar en la Figura 4-12.

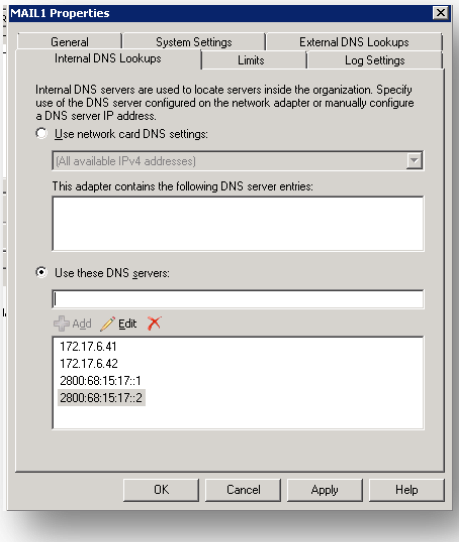

Figura 4-12. Configuración de los DNS internos para el correo
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

- Y finalmente se debe agregar en la consola del Exchange 2007 en las propiedades de transporte las direcciones IPv6 de los equipos que pueden realizar SMTP para el envío de correo desde la red interna.

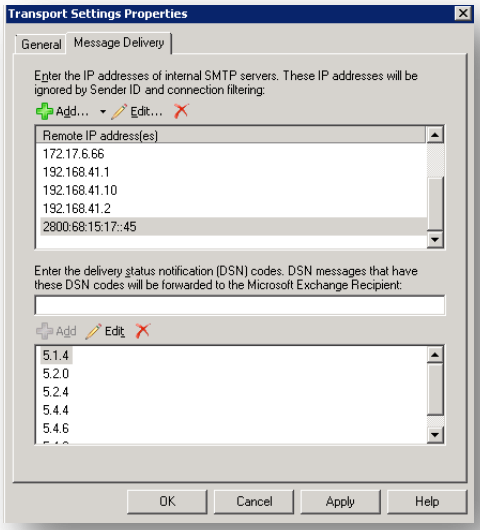

Figura 4-13. Configuración de direcciones IPv6 para permisos *smtp*
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.2.1.4 Configuración en el Equipo de *Core*6506

El equipo de *Core* es un equipo robusto de marca cisco y modelo WS 6506, este equipo maneja todo el tráfico de la red interna administrativa y realiza función de enrutamiento inter *vlan* y envía todo el tráfico hacia el firewall, inclusive maneja el tráfico de las sedes hacia los servidores web y da acceso a internet excluyendo a Guayaquil, Santo Domingo y Salinas que tiene sus propios enlaces.

Las configuraciones que se realizaron en este equipo son las siguientes:

- En la interface *GigabitEthernet* 3/26 del equipo se asignó una dirección IP 2800:68:15:1::3 ya que por esta interface se ruteará todo el tráfico hacia el *firewall* como se puede observar en la Figura 4-14.

```
interface GigabitEthernet3/26
 description PUENTE-IPS
 ip address 192.168.0.3 255.255.255.240
 ip access-group IDS_gi3/26_in_1 in
 ip access-group IDS_gi3/26_out_1 out
 ipv6 address 2800:68:15:1::3/64
 no cdp enable
 service-policy input IDS_RL_POLICY_MAP_1
 service-policy output IDS_RL_POLICY_MAP_1
```

Figura 4-14. Configuración IPv6 en la interface de conexión al Firewall
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

- En la Interface de la vlan de administración se asignó la dirección 2800:68:15:15::254, se habilito IPv6 con el comando IPv6*enable*y se añadió las líneas IPv6*traffic-filter* test *in /out* para permitir el tráfico de entrada y salida como se puede observar en la Figura 4.15.

En la vlan administrativo o cualquier vlan que se defina en el core, hay que poner los mismos comandos y solo se cambiará la dirección IPv6 que corresponde a cada vlan, por ejemplo para la vlan 3 administrativo se asignó la IPv6 2800:68:15:17::254, que servirá de Gateway o puerta de enlace a cada vlan.

```
interface Vlan1
 ip address 192.168.15.254 255.255.255.0
 ipv6 address 2800:68:15:15::254/64
 ipv6 enable
 ipv6 traffic-filter test in
 ipv6 traffic-filter test out
```

Figura 4-15. Configuración IPv6 en la vlan de administración
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

- En la Figura 4-16 se puede observar la configuración de la rutas por defecto y el protocolo *OSPF (Open Short PathFirst)* que se levantó para permitir la comunicación entre *vlans* y el encaminamiento hacia internet.

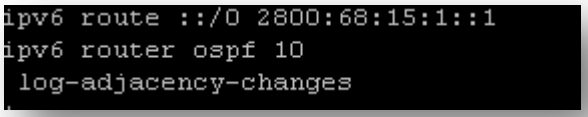

Figura 4-16. Configuración de la ruta por defecto
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

- Se creó también una lista de acceso que permite la circulación del tráfico IPv6 sin restricciones como se puede observar en la Figura 4-17.

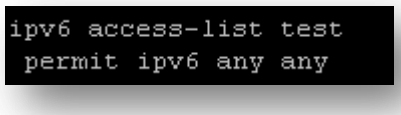

Figura 4-17. Comandos para agregar las listas de acceso
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.2.1.5 Configuración en los Equipos *Switches* de Acceso

En el capítulo III se pudo concluir que los equipos que se manejan en la Universidad a nivel nacional son los Switches cisco 2960, por lo tanto se enfocará en la configuración de los mismos tomando en cuenta que los comandos y el procedimiento se lo realizará de la misma manera para todos.

- Para la configuración los equipos cisco se debe tener actualizado el IOS a la versión 12.2 (44) 7 como mínimo. Una vez actualizados se ejecuta el comando **sdmprefer dual-IPv4-and-Ipv6default**como se observa en la Figura 4-18, esto permite que el *Switch* soporte IPv6 y pueda seguir manejando IPv4 al mismo tiempo.

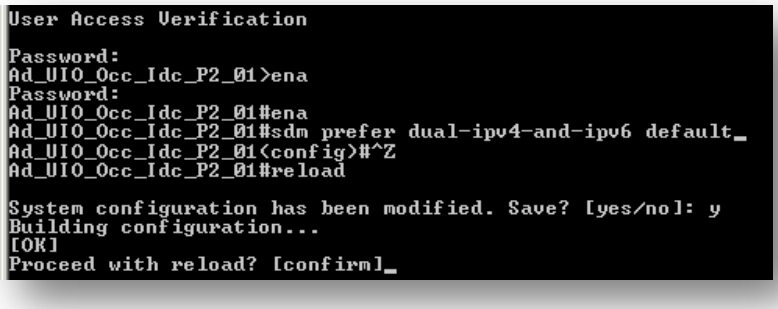

Figura 4-18. Comandos para activar en un *switch* 2960, Dual IPv4eIPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

- En la Figura 4-19 se tiene la configuración para asignar una dirección IPv6 a un *Switch* para poderlo identificar y administrarlo por red.

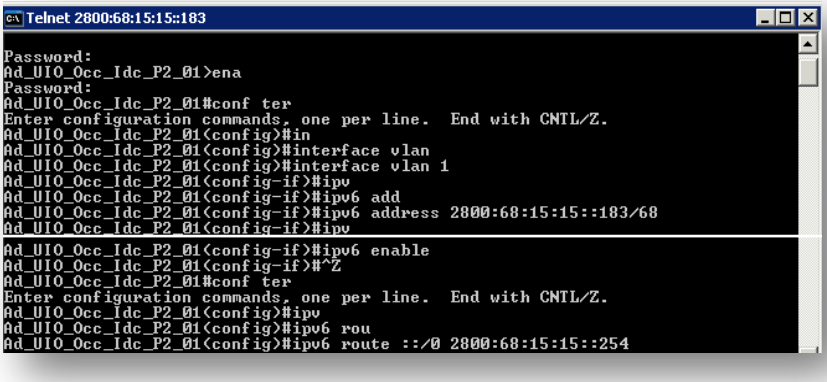

Figura 4-19. Configuración de la IPv6 de administración y la Ruta en los *Switches* 2960
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

[7]http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_53_se/configuration/guide/swIpv6.html#wp1216629

4.2.1.6 Configuración en los Computadores de la red

En la Universidad Tecnológica Equinoccial se manejan los sistemas operativos actualizados y como se pudo analizar en el Capítulo III, las versiones instaladas son Windows 7 y Windows 2008 server en la mayoría de estaciones, los sistemas que se tienen instalados son:

- Windows 2003 y 2008 Server
- Windows Xp
- Windows Vista y 7
- Linux
- MacOs

A continuación se presenta la implementación del protocolo IPv6 sobre estos sistemas operativos.

4.2.1.6.1 Configuración sobre equipos Windows 2003 server y Windows XP

Debido a que Windows 2003 y Windows XP tiene más o menos la misma generación, la instalación se realiza de la misma manera.

1. Se habilita IPv6, con una cuenta de usuario con privilegios para cambiar la configuración de red. desde una ventana de comando se ejecuta: *netsh interface IPv6install.*

Figura 4-20. Pantalla configuración DNS Principal
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Otra forma de habilitar IPv6 es desde Conexiones de red, en la tarjeta de red se selecciona Propiedades -> Instalar -> Protocolo -> Agregar. Selecciona IPv6 y finalmente Aceptar.

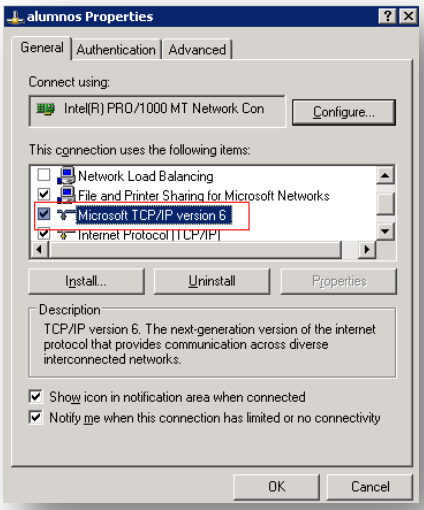

Figura 4-21. Configuración para habilitar IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

2. Para asegurarse que IPv6 está instalado y funciona correctamente se ejecuta en una ventana de consola: **ping ::1**

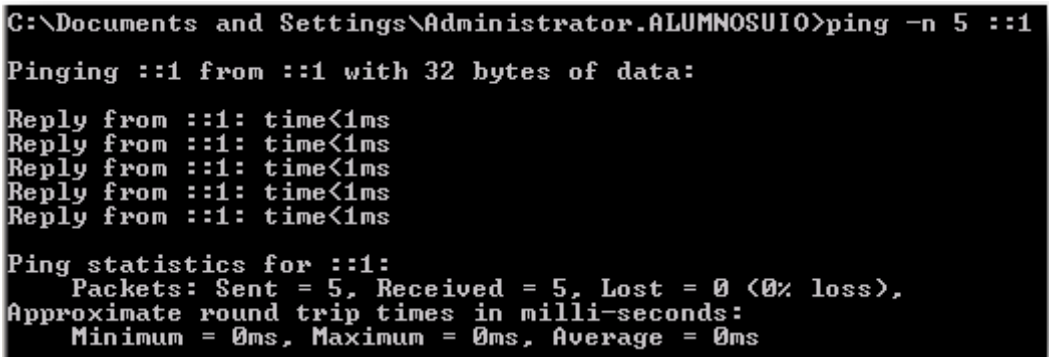

Figura 4-22. Confirmación de instalación IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

3. Se abre la ventana del símbolo del sistema y se ejecuta el comando **dnscmd /config /EnableIpv6 1**

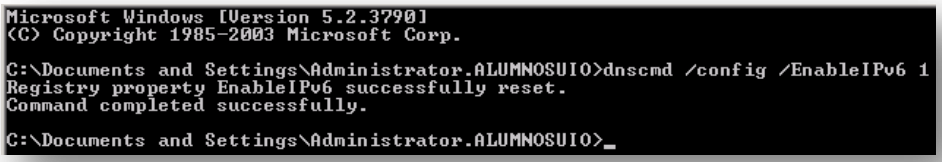

Figura 4-23. Ejecución del comando *Enable*IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Se reinicia el servicio Servidor DNS.

4.2.1.6.2 Configuración sobre equipos Windows 2008, Windows Vista y Windows 7.

La configuración de IPv6 en los sistemas operativos *Windows* Vista, Win*d*ows 2008 *server* y *Windows* 7 es una funcionalidad nativa e incluyen un buen soporte del protocolo IPv6, no solo de características básicas como en Windows como Windows XP y Windows 2003, si no también características avanzadas como:

- Doble pila IPv4/IPv6
- Interfaz gráfico de usuario (GUI)
- Soporte completo para *IPsec*
- Protocolo *Multicast*MLDv2
- Resolución de Nombres *Multicast* por acceso local LLMNR
- Direcciones IPv6 literales en las URLs
- Soporte de IPv6 en conexiones PPP
- DHCPv6
- Identificadores de interfaz aleatorios

En estos sistemas operativos el protocolo IPv6 ya está configurado y habilitado por defecto. A pesar de esto se pueden configurar algunas características de IPv6 tal y como se explica en los siguientes pasos.

1. En propiedades de red se escoge la opción de IPv6 que viene habilitado por omisión, para asignar las configuraciones manualmente.

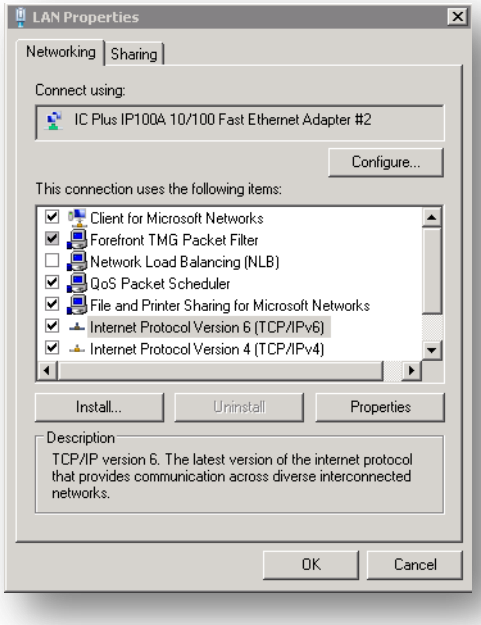

Figura 4-24. Propiedades de red con soporte IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

2. Se ingresa la dirección IPv6 de acuerdo al rango asignado para la red administrativa, aunque en la mayoría de computadores con estas versiones de sistemas operativos toman automáticamente la IPv6 del DHCPv6.

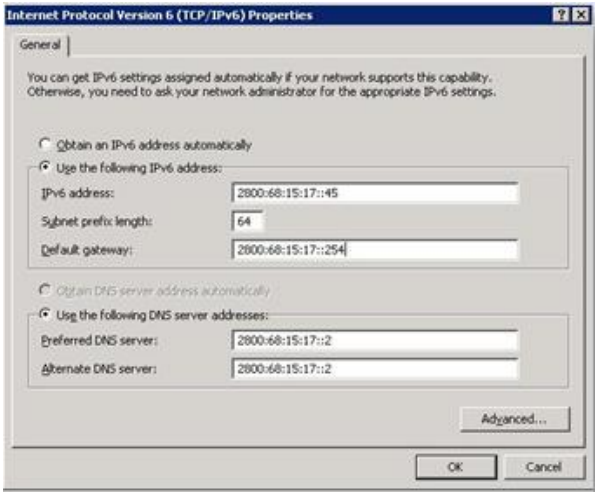

Figura 4-25. Asignación manual de IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En estos sistemas operativos se puede realizar otros comandos que ayudan a realizar ciertas comprobaciones, los mismos que se detallan en el Anexo 7.1.

4.2.1.7 Configuración de IPv6 en las impresoras de Red

En el Capítulo III se analizó que la mayoría de impresoras de red soportan en su sistema operativo IPv6, a continuación se expone la configuración de una impresora como ejemplo.

1. Se habilita el protocolo IPv6 ya que por omisión está deshabilitado como se puede observar en la Figura 4-26.

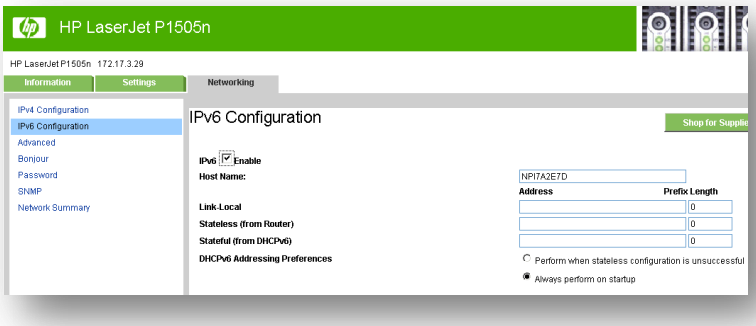

Figura 4-26. Habilitación de IPv6 en una impresora de red
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

2. En la Figura 4-27 se puede visualizar la dirección IPv6 asignada por el estado del *router* que corresponde al rango asignado a la red administrativa

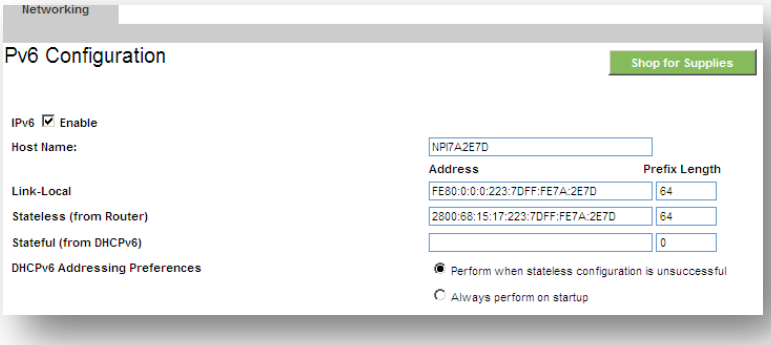

Figura 4-27. Asignación automáticaIPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Desde cualquier estación de la red administrativa se puede comprobar la conectividad a esa dirección como se puede observar en la Figura 4-28

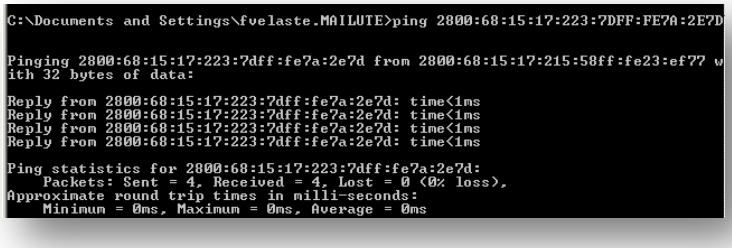

Figura 4-28. Comprobación de conexión a la impresora
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

La configuración desde la estación de trabajo, se realiza de la misma manera como se configura en IPv4, con la diferencia que la IP es v6, en la Figura 4-29 se visualiza la IPv6 asignada que corresponde a la impresora de red.

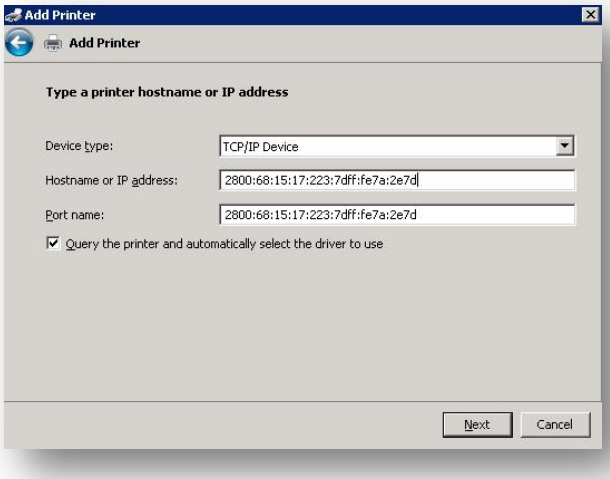

Figura 4-29. Configuración de la impresora en el cliente
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Una vez configurada la impresora, las configuraciones quedarían como se observa en la Figura 4-30.

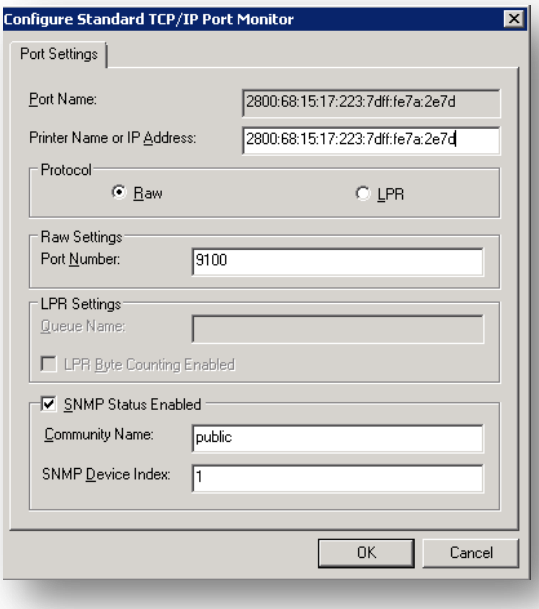

Figura 4-30. Comprobación de las configuraciones de la impresora
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la Figura 4-31 se tiene la orden de impresión de la página de prueba enviada desde la estación de trabajo y se puede observar que toda la comunicación es a través de IPv6.

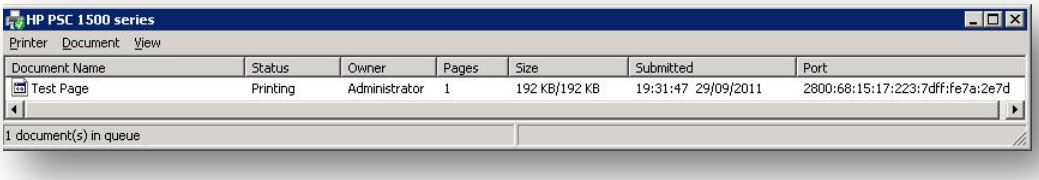

Figura 4-31. Impresión de la página de prueba con IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.2.1.8 Configuración IPv6 en la Cámaras IP

Como se dedujo en el Capítulo III, en la Universidad se han implementado al momento 328 cámaras IP marca Axis, se tiene planificado también para el futuro incrementar en un 70 % el número de las mismas. Todas soportan el protocolo IPv6 pero ciertas cámaras no se pueden configurar manualmente ya que no tiene una interface gráfica por lo que solo tomarán una IP dinámicamente.

En la Figura 4-32 se puede observar cómo se habilita IPv6 en las cámaras que por omisión viene deshabilitada, y estaría configurado para que soporte este protocolo.

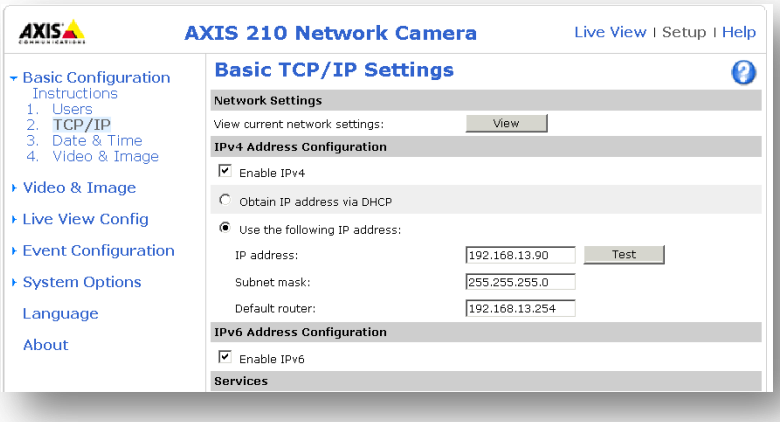

Figura 4-32. Habilitación de IPv6 sobre las cámaras IP
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.2.1.9 Configuración de IPv6 en el Servidor de Antivirus

En la Universidad se maneja como servidor antivirus el *endpoint*, que a través de ciertas políticas de red permite el bloqueo de virus y tráfico malicioso, pero hay que tomar en cuenta que en las políticas por omisión del módulo del firewall de este antivirus, que se aplican a un grupo de máquinas; el trafico IPv6 está bloqueado, en la Figura 4-33 se indica la configuración de la misma para permitir este tráfico.

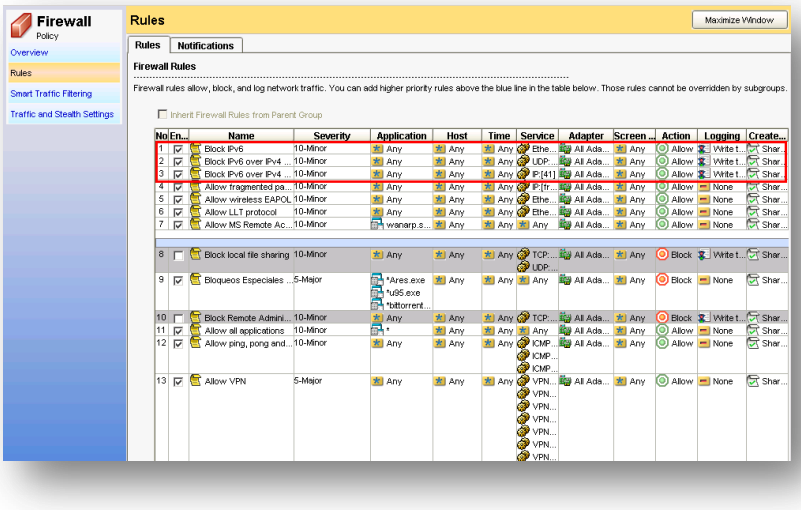

Figura 4-33. Configuraciones en el firewall del servidor de antivirus
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.2.2 Implementación de IPv6 sobre la red Alumnos

En el Capítulo III se identificó la estructura de las redes internas de la Universidad, en donde se menciona que la red de alumnos está físicamente separada de la red administrativa, y para mantener los estándares se manejan los mismos dispositivos y aplicaciones. Por tal motivo se expone solo las configuraciones de los dispositivos y servicios complementarios que no se repetirán y que ya se mencionaron en las configuraciones de la red administrativas de la sección4.2.1.

Los servicios que se mencionarán son:

- Configuración en el Equipo de *Core*4500
- Configuración en los equipos Inalámbricos (*Wireless)*

4.2.2.1 Configuración en el Equipo de *Core*4500

Este equipo marca cisco y modelo WS 4503 al igual que en la red de administrativos maneja todo el tráfico de la red de alumnos y realiza la función de enrutamiento inter vlan y envía todo el tráfico de Internet hacia el mismo firewall que se maneja para todas las redes internas.

Las configuraciones que se realizaron en este equipo son las siguientes:

- En la interface *Port-channel2* del equipo se asignó una dirección IP 2800:68:15:3::30 para que se envíe todo el tráfico hacia el firewall como se puede observar en la Figura 4-34.

```
interface Port-channel2
 description PORT-CHANNEL LAN_AL-FORTINET
 ip address 192.168.0.30 255.255.255.252
 ipv6 address 2800:68:15:3::30/64
 ipv6 enable
 no ipv6 mfib fast
```

Figura 4-34. Configuración IPv6 en la interface de conexión al Firewall
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

- En la Interface de la *vlan* de administración se asignó la dirección 2800:68:15:15::253, se habilitó IPv6 con el comando *IPv6enable* y se

añadió las líneas *IPv6traffic-filter test in /out* para permitir el tráfico de entrada y salida como se puede observar en la Figura 4.35.

- En la *vlan* 2 se asignó la IPv6 2800:68:15:16::4, que servirá de Gateway o puerta de enlace a toda la red de alumnos 2800:68:15:16::

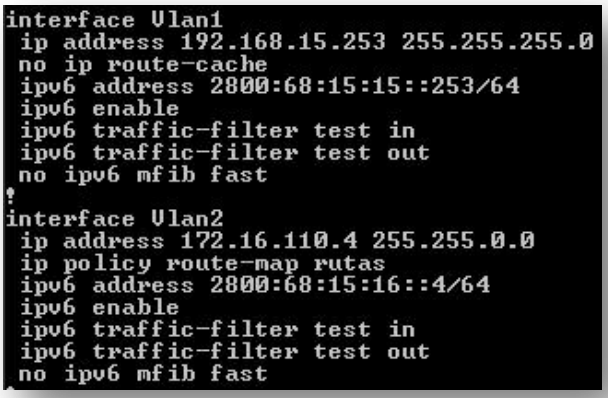

Figura 4-35. Configuración IPv6 en las *vlan*
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

- En la Figura 4-36 se puede observar la configuración de las rutas por omisión que se levantó para permitir la comunicación entre vlans y el encaminamiento hacia internet.

Figura 4-36. Configuración de la ruta por omisión
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

- Se creó también una lista de acceso que permite la circulación del tráfico IPv6 sin restricciones como se puede observar en la Figura 4-37.

```
ipv6 access-list test
 permit ipv6 any any
```

Figura 4-37. Comandos para agregar las listas de acceso
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.2.2.2 Configuración de IPv6 en la red inalámbrica (*wireless*)

Para habilitar la red inalámbrica se procedió con la siguiente configuración:

- Se asignó la dirección IPv6 2800:68:15:10::1 en la *vlan* 9 correspondiente a la red inalámbrica, que será utilizada como la puerta de enlace.

```
!
interface Vlan9
 ip address 10.10.10.1 255.255.0.0
 ip policy route-map rutas
 ipv6 address 2800:68:15:10::1/64
 ipv6 enable
 ipv6 traffic-filter test in
 ipv6 traffic-filter test out
 no ipv6 mfib fast
```

Figura 4-38. Configuración del ruteo en la *vlan* de la red inalámbrica
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Luego de esta configuración, lo único que se tiene que realizar es la configuración en el cliente, tomando en cuenta que si ya tiene en su sistema operativo soporte para IPv6, no se debería configurar nada.

La configuración en el cliente como la puede visualizar en las figuras 4-39 y 4-40.

En la Figura 4-39 se observa la conexión y configuración a la red inalámbrica UTE_ON_AIR en donde se ha asignado una IPv6.

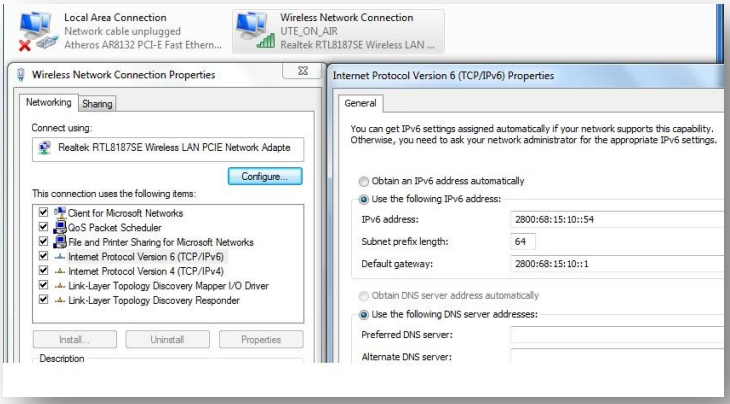

Figura 4-39. Configuración de IPv6 en la red inalámbrica del cliente
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la Figura 4-40 se puede visualizar y comprobar la conectividad IPv6, se ha realizado un ping hacia el *router* desde un cliente inalámbrico y el navegador indica la ventana de bienvenida al servicio inalámbrico.

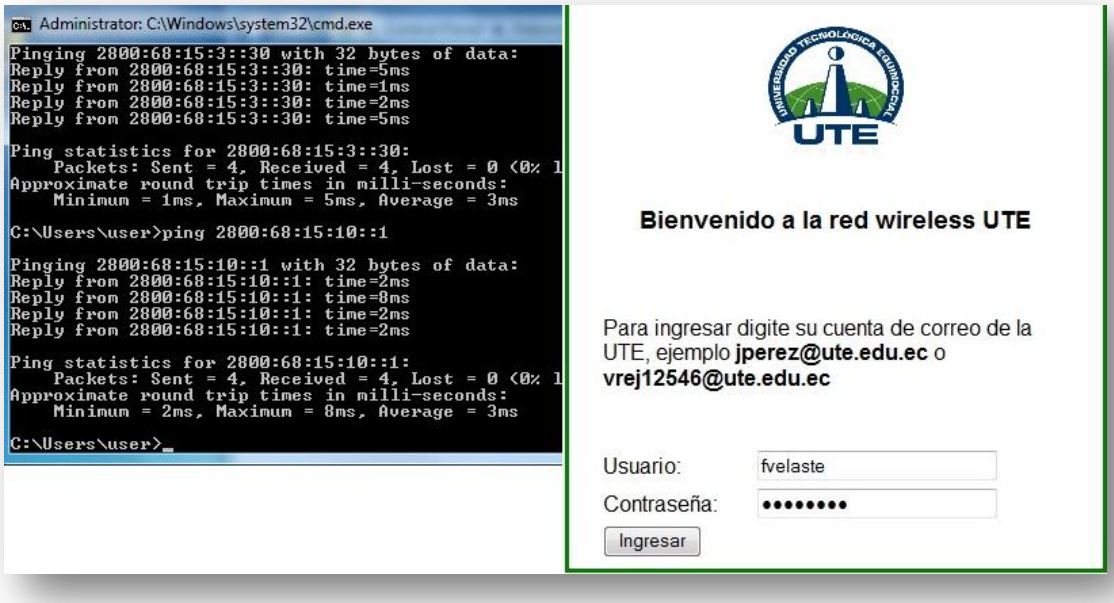

Figura 4-40. Navegación desde la red inalámbrica por IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.2.3 Implementación de IPv6 sobre la WAN

Con base en el diagrama presentado en el Capítulo III, en el que se detalla la estructura de la red WAN se rediseña el esquema con la configuración y direccionamiento IPv6.

En la Figura 4-41 se expone la configuración del direccionamiento IPv6 aplicado en la WAN, se ha tratado de mantener una relación con el direccionamiento IPv4, es decir si por ejemplo en Ambato el direccionamiento en IPv4 es 192.168.100.x en IPv6 es 2800:68:15:100::x.

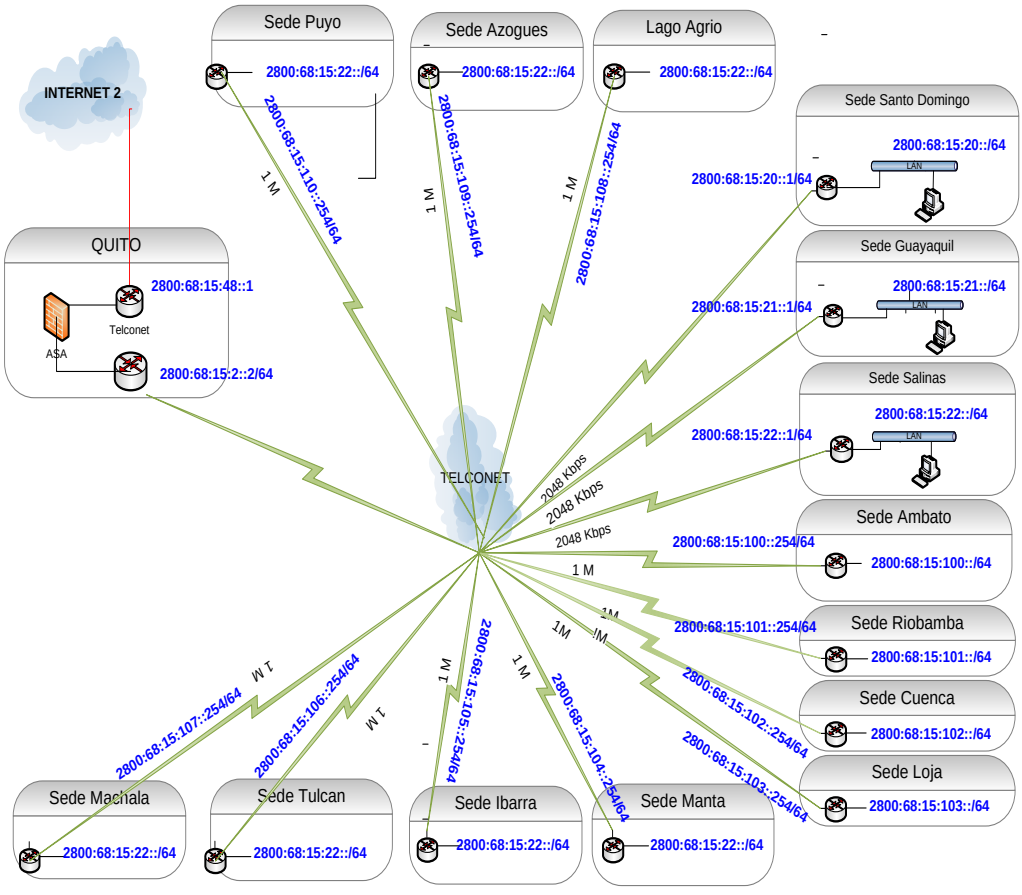

Figura 4-41. Esquema del direccionamiento IPv6 de la red WAN
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Hay que tomar en cuenta que en las sedes y centros de apoyos ubicados en las diferentes provincias del Ecuador, se manejan los mismos equipos y aplicaciones que en el Campus Quito, por tal razón solo se mencionará la configuración de los siguientes equipos:

- *Router* 2800
- *Firewall Fortinet* 1240 B

Existen otros equipos que son parte de la WAN, pero sus configuraciones dependen del proveedor ya que son administrados por ellos.

4.2.3.1 Configuración en el *Router* que va hacia las Sedes

En la Figura 4-42 se observa la asignación de la dirección IPv6para el*router* que interconecta todos los enlaces de la WAN

Figura 4-42. Configuración IPv6 sobre la interface física hacia proveedor
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la Figura 4-43 se tiene la configuración en donde se asigna la dirección IPv6 para la *vlan* de administración del *router* y los comandos IPv6*traffic-filter test out* / *in* que permiten el paso del tráfico de IPv6 tanto de entrada como de salida.

```
interface Vlan1
 description LAN de la UTE
 ip address 192.168.0.2 255.255.255.240
 ip policy route-map trafico
 load-interval 30
 ipv6 address 2800:68:15:1::2/64
 ipv6 enable
 ipv6 traffic-filter test in
 ipv6 traffic-filter test out
```

Figura 4-43. Configuración de IPv6 sobre la *vlan* de administración
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la Figura 4-44 al igual que el *Switch* de *Core* de administrativos se crea la lista de acceso para permitir cualquier protocolo IPv6.

```
ipv6 access-list test
 permit ipv6 any any
```

Figura 4-44. Comandos para las listas de acceso en IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.2.3.2 Configuración en el Equipo Firewall

El *firewall* Fortinet 1240B es un modelo actual con soporte IPv6, las configuraciones se han realizado a base de las interfaces que se muestran en la Figura 4-45, en las que están definidas las redes internas y externas de la Universidad.

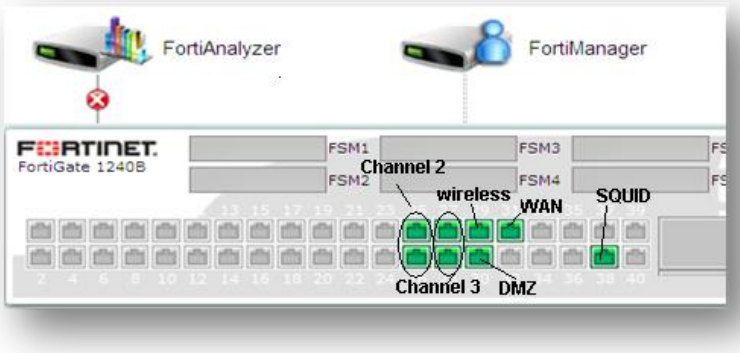

Figura 4-45. Interfaces levantadas en el firewall sobre IPv6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

La configuración sobre las interfaces *EtherChannel* (*Channel* 2 y *Channel3*) se realizó por línea de comandos, ya que desde la interface gráfica GUI no funciona bien, para las otras interfaces simples la configuración aplicada es por GUI.

Configuración *Channel* 2

```
next
edit "Channel 2"
    set vdom "root"
    set ip 192.168.0.1 255.255.255.240
    set allowaccess ping https ssh
    set type aggregate
        set member "port25" "port26"
    set description "interface lan administrativa"
        config ipv6
            set ip6-address 2800:68:15:1::1/64
            set ip6-allowaccess ping
        end
```

Figura 4-46. Configuración por línea de comandos para *channel2*
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Configuración *Channel* 3

```
    next
    edit "Channel 3"
        set vdom "root"
        set ip 192.168.0.29 255.255.255.252
            set allowaccess ping https ssh
        set type aggregate
            set member "port27" "port28"
        set description "interface lan alumnos"
            config ipv6
                set ip6-address 2800:68:15:3::17/64
            end
    next
end
```

Figura 4-47. Configuración por línea de comandos para *channel3*
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Configuración para las interfaces simples

Para activar y configurar una dirección IPv6 en las interfaces simples del Fortinet se coloca la dirección manualmente por la interface gráfica como se observa en la Figura 4-48.

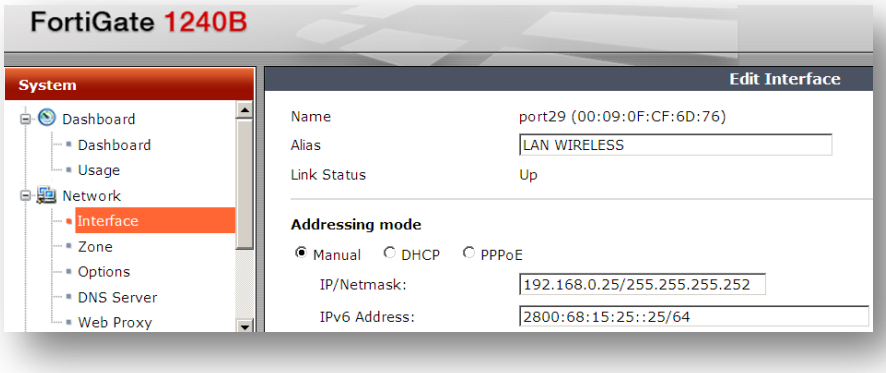

Figura 4-48. Configuración para las interfaces simples por GUI
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Configuración de accesos

Para poder administrar el equipo a través de esta interface se habilita los protocolos *https*, *http* y ping.

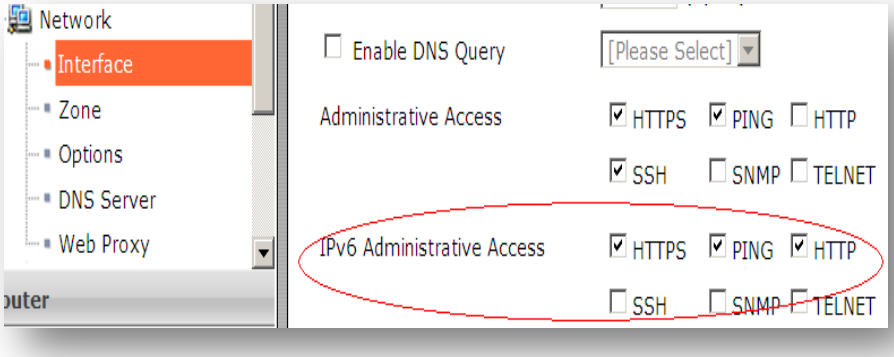

Figura 4-49. Configuración de accesos a las interfaces
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

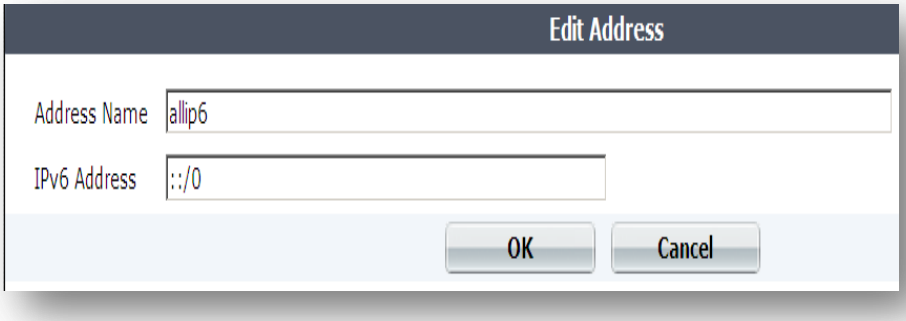

Figura 4-50. Política de acceso allip6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Se crea la política de acceso allip6 para que cualquier red ::/0 pueda acceder desde afuera o desde adentro por IPv6.

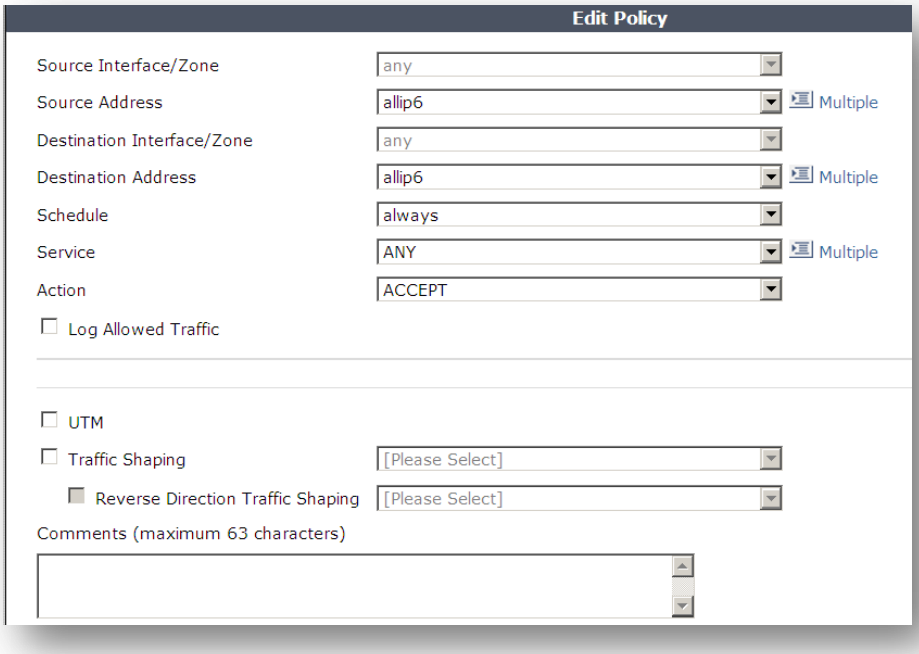

Figura 4-51. Políticas aplicadas para accesos
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Configuración de las Rutas

En la Figura 4-52 se define la ruta para que la red administrativa 2800:68:15:17:: tenga como default *router* la dirección IPv6 2800:68:15:1::3 /64

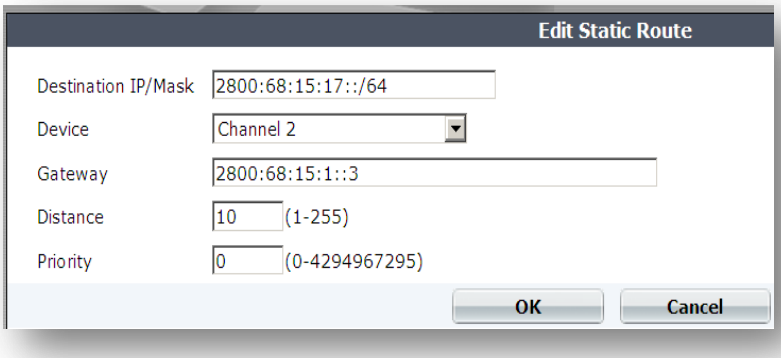

Figura 4-52. Configuración de las rutas de estáticas
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la Figura 4-53 se visualiza como se asigna una ruta IPv6 a través de comandos en CLI del Fortinet.

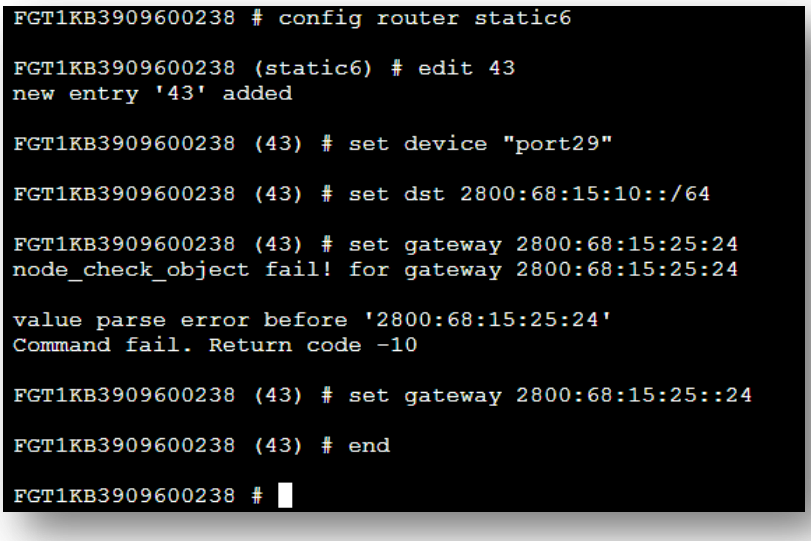

Figura 4-53. Configuración de una ruta por línea de comandos
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Y finalmente podemos observar en la Figura 4-54 las rutas configuradas de acuerdo a las redes internas o declaradas en el Fortinet.

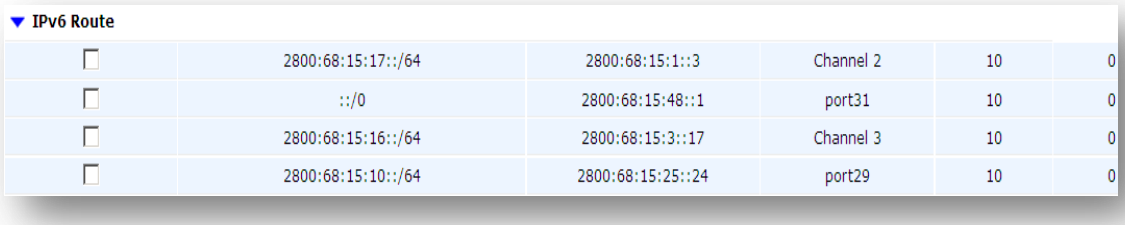

Figura 4-54. Rutas estáticas aplicadas
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.3 RESULTADOS DE LA IMPLEMENTACIÓN IPv6 vs IPv4

A continuación se presenta los resultados que verifican la conexión IPv6 hacia el Internet y el tráfico generado en la intranet comparándolo con IPv4.

En la figura 4.55 se muestra el resultado de la navegación hacia un servidor que se encuentra en Estados Unidos, este servidor devuelve la direcciones IPv6 y IPv4 que tiene configurado el equipo, que para este ejemplo se encuentra en la intranet de la Universidad, con lo que se entiende que ambos protocolos están habilitados.

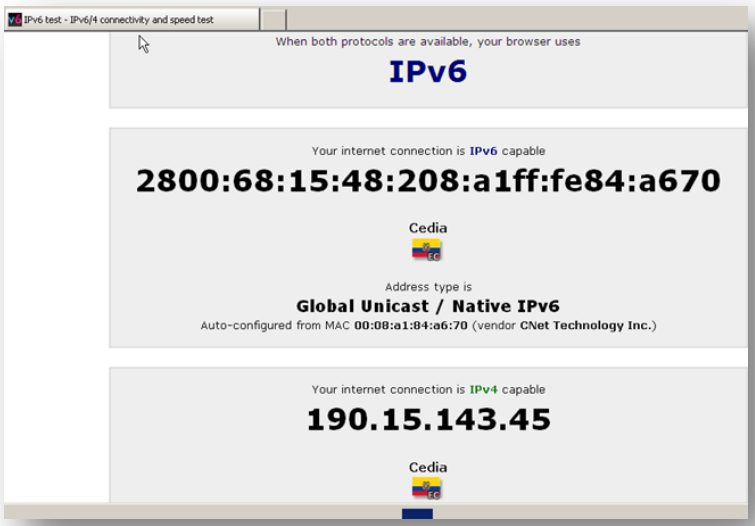

Figura 4-55. Prueba de conexión con IPv4 e IPv6
Fuente: http://www.ipv6-test.com/
Elaborado por: El Autor

En la figura 4.56, a través de este mismo servidor en Estados Unidos, se valida la configuración del servidor web (www.ute.edu.ec) implementado con IPv6 bajo la plataforma *Internet Information Service* Versión 6.0 (IIS 6.0) en Windows 2008

Server, se observa una correcta configuración del servidor web y sus registro DNS.

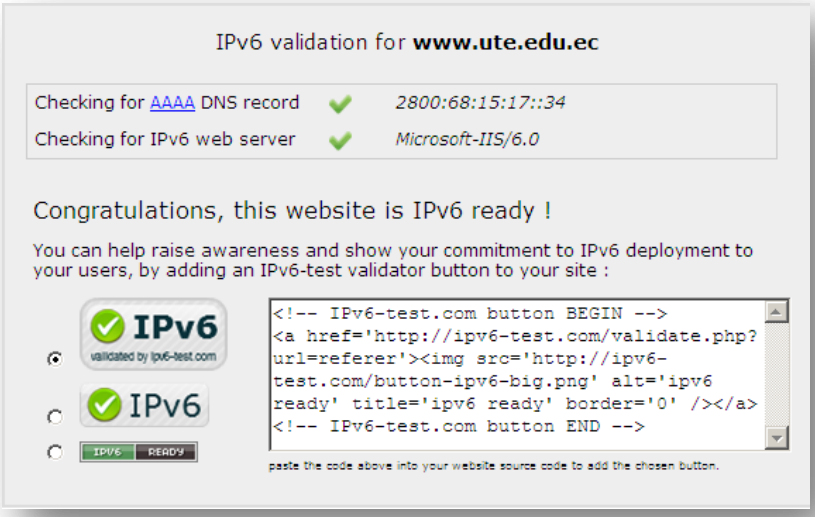

Figura 4-56. Validación del sitio web de la UTE
Fuente: http://www.ipv6-test.com/
Elaborado por: El Autor

4.3.1 Captura y análisis de paquetes

Con la herramienta *Wireshark* versión 1.6.5 con soporte IPv6, se realiza el análisis de tráfico, en el ejemplo se captura los paquetes tanto en IPv4 como en IPv6 que realizan la misma tarea, con el objetivo de compararlos y comprobar sus diferencias

En la figura 4.57, se observa las tramas IPv4 e IPv6, capturadas a nivel de capa 2, en donde se ha resaltado en un círculo rojo, los datos que son diferentes, para este caso solo se verifica que el protocolo y tipo de los *frames* se cambian de IPv4 a IPv6, esto es correcto ya que a este nivel no hay más cambios y prácticamente tienen los mismos campos y encabezados.

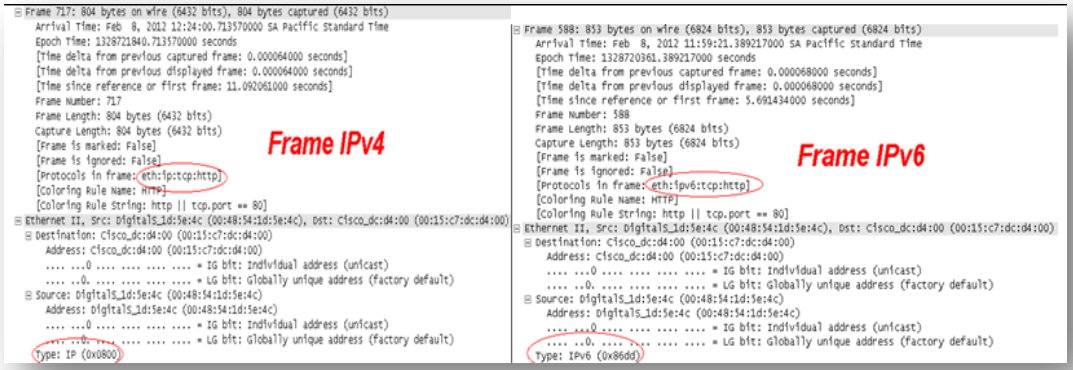

Figura 4-57. Frame IPv6 vs IPv4
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la figura 4.58, se tiene la captura de los paquetes IPv4 e IPv6 a nivel de capa 3, en donde algunos campos ya cambian, resaltados en círculos rojos se tienen los campos que se mantienen, aunque por ejemplo el campo versión, cambia de 4 a 6; subrayados de color azul son los campos que desaparecen, subrayados de color verde son los campos que se aumentan para IPv6, y se puede observar el campo de clase de tráfico que es mejorado par el nuevo protocolo v6.

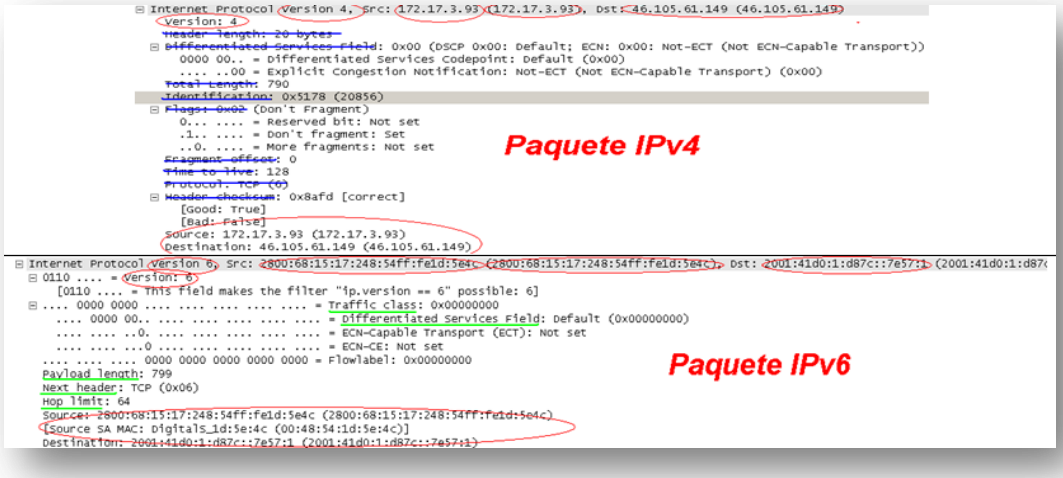

Figura 4-58. Paquete IPv6 vs IPv4
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la figura 4.59, se muestra los segmentos IPv4 e IPv6 a nivel de capa 4, aquí se manejan los mismos campos, con la única diferencia que se ha aumentado el campo de análisis SEQ/ACK, que permite ser al protocolo IPv6 de confiabilidad mejorado que IPv4.

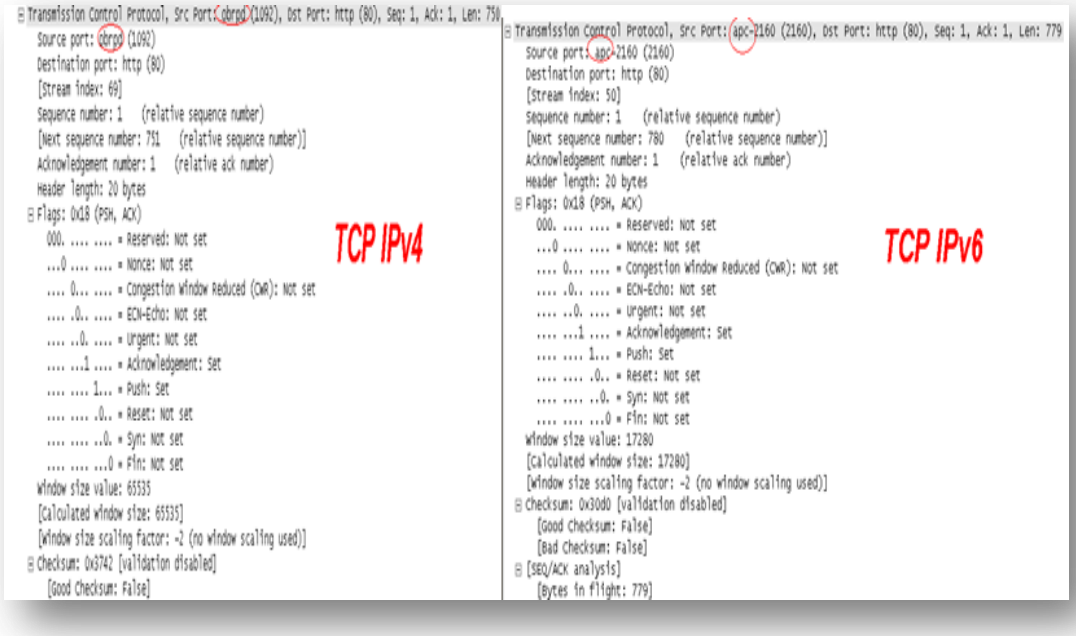

Figura 4-59. Segmentos TCP v4 vs v6
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la figura 4.60, se puede observar que se mantienen los encabezados a nivel de aplicación, con la única diferencia que los URL se direccionan a los correspondientes códigos de IPv6 o IPv4 implementados en el servidor web.

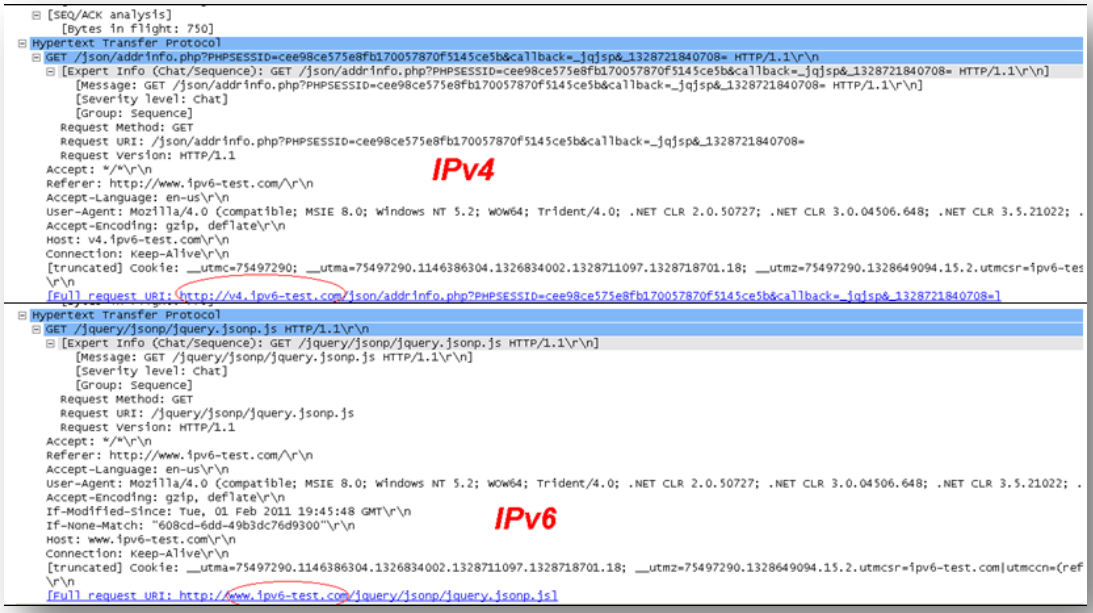

Figura 4-60. Aplicación http
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.3.2 Tiempos de respuesta y rutas

Se ha analizado los tiempos de respuesta y rutas generadas, al enviar un paquete *icmp* desde la red interna hacia el internet en IPv4 e IPv6, obteniendo las siguientes gráficas de resultados:

En la figura 4.61, se puede observar el tiempo que se demora en viajar un paquete *icmp* (ping) hacia un servidor de internet, para la IPv6 el tiempo promedio es 179 ms y 0 % de pérdidas y para la IPv4 debido a que se utiliza NAT y realmente es la dirección pública 192.188.51.31 con la que navega este rango de

equipos, no se tiene acceso a la dirección privada del equipo, cabe recordar que en IPv6 ya no existe el NAT.

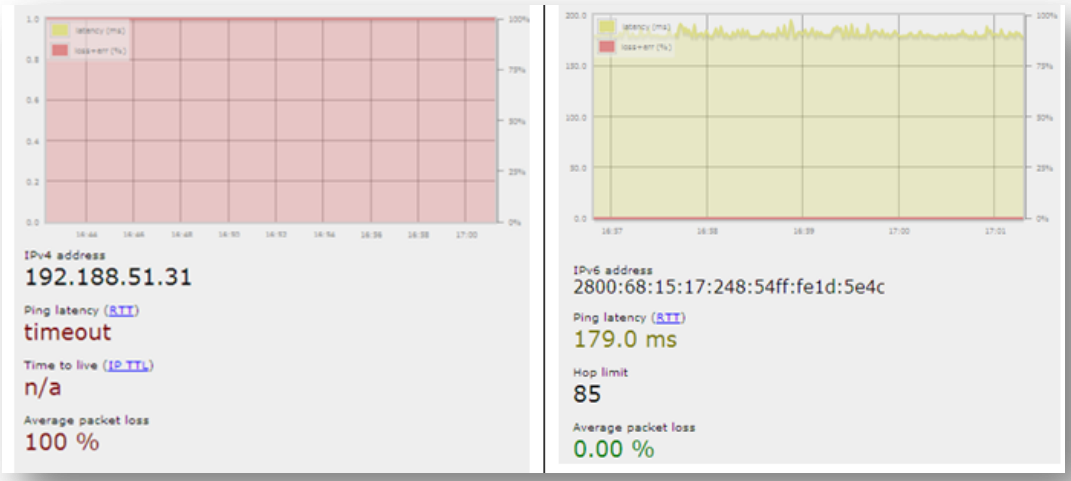

Figura 4-61. Retardo del paquete ping red interna
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

Para poder realmente comparar el tiempo de respuesta entre los dos protocolos se configuró un equipo con una IPv4 pública de Internet 2, que a través de CEDIA se asignó este rango de direcciones a la Universidad.

Como se puede observar en la figura 4.62; para la IPv4 190.15.143.45/24 el tiempo de respuesta promedio es 186.1 ms y 0% de pérdida, para la IPv6 2800:68:15:48:208:a1ff:fe84:a670/64 el tiempo de respuesta es 190.9 ms y 0% de pérdida, los dos paquetes toman el mismo camino y prácticamente el mismo tiempo, pero para IPv6 luego de varias capturas, los picos en las gráficas son muy constantes a diferencia de IPv4 que existe gran variación.

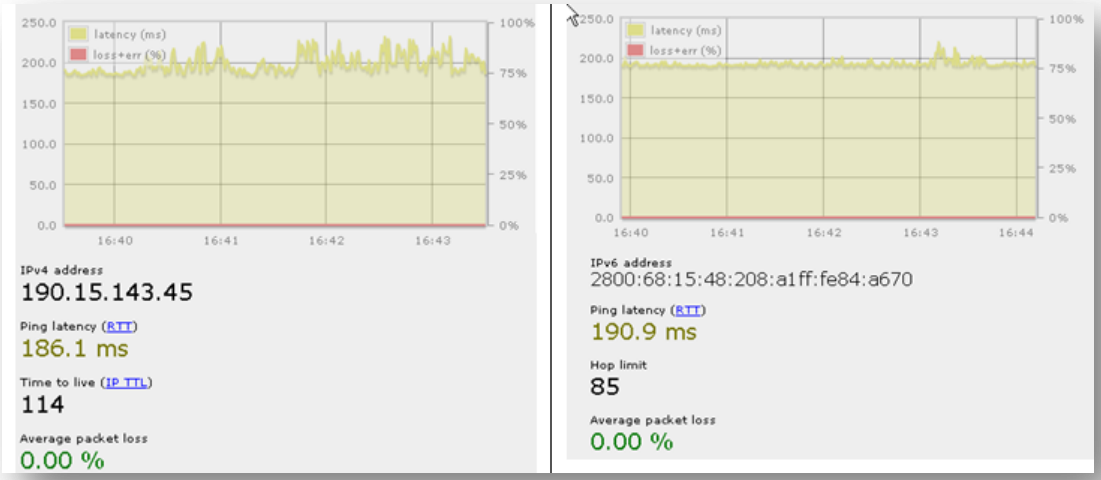

Figura 4-62. Retardo del paquete ping red externa
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la figura 4.63, se presenta el resultado del comando ping tanto IPv4 como IPv6, este paquete viaja desde un servidor del internet hacia los servidores en nuestra red interna, verificando que para IPv6 la latencia es menor que en IPv4.

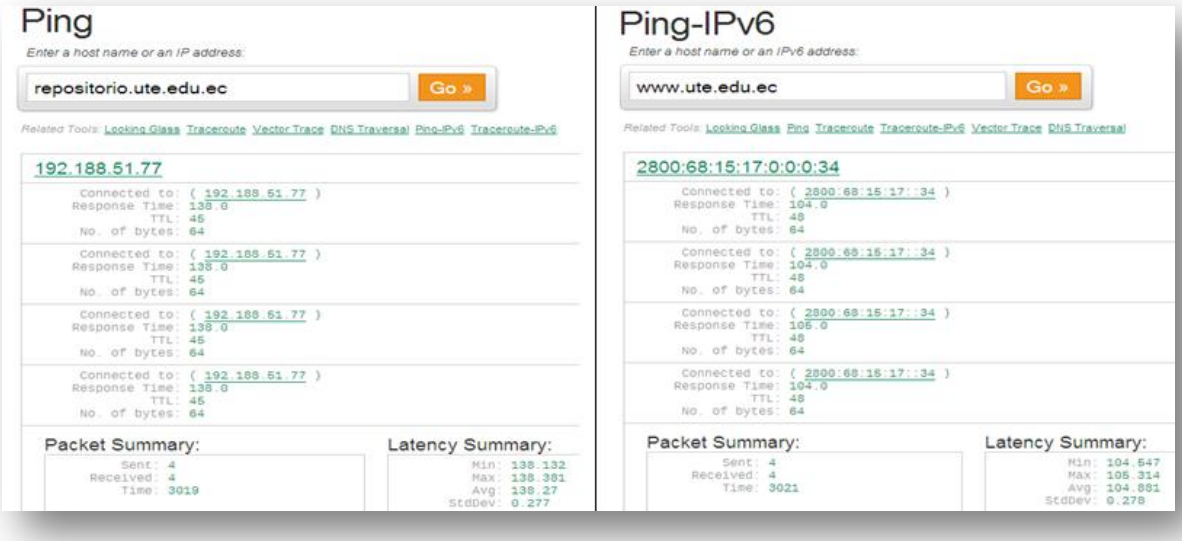

Figura 4-63. Retardo del ping desde la red Internet hacia la red externa
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la figura 4.64, se muestra la ruta con los saltos que se generan desde el internet hacia el servidor web de la Universidad, obteniendo tanto para IPv4 como IPv6; diecisiete saltos, tomando en cuenta que para IPv4 por el *NAT* el paquete *traceroute* no llega a su destino ya que la dirección es reservada.

Figura 4-64. Rutas desde Internet hacia la red interna
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

4.3.3 Monitoreo del Tráfico

El monitoreo se lo ha realizado en el firewall principal (FORTINET) y para sacar los gráficos se ha utilizado el reporteador (FORTIANALYZER), que ha permitido sacar reportes individuales clasificando el tráfico IPv4 del IPv6.

Figura 4-65. Cabeceras de los reportes generados
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la figura 4.66 se puede observar que los principales servicios que se manejan en IPv4 e IPv6 son TCP, aunque debido que IPv4 es inseguro se maneja mucho el protocolo 443

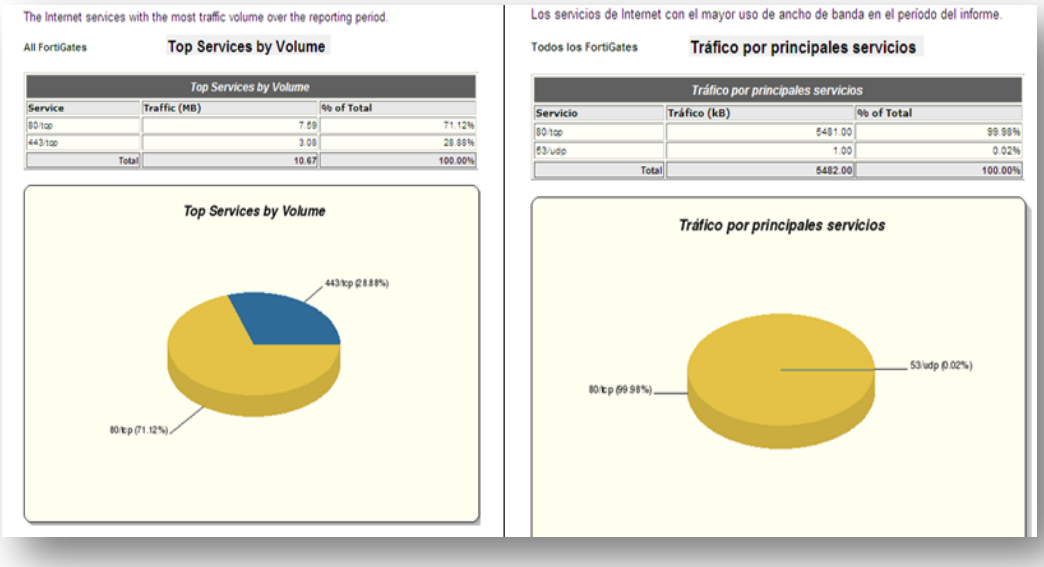

Figura 4-66. Principales servicios
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la figura 4.67, como el reporte se generó desde un mismo origen, solo se visualiza la dirección IPv4 como la IPv6 del mismo.

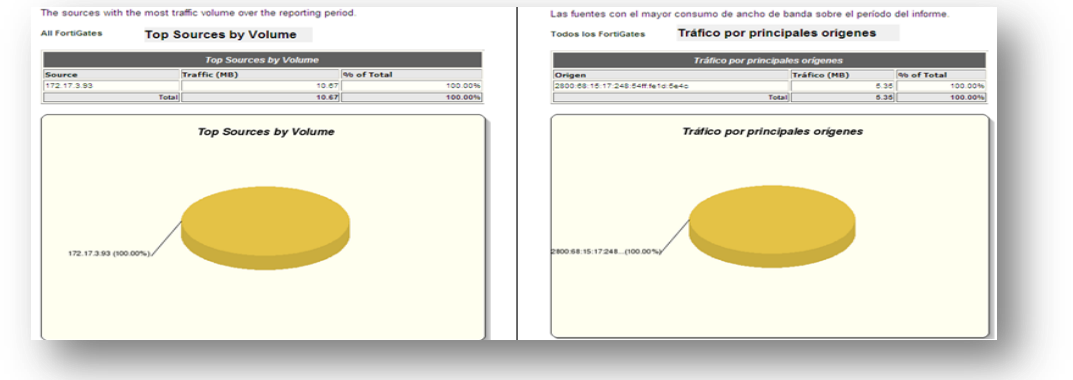

Figura 4-67. Principales Origenes
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

En la figura 4.68, se presenta un reporte de las direcciones destinos tanto en IPv4 como IPv6 hacia el internet, observando que el tamaño de tráfico IPv6 es mucho menor, esto hace notar que los canales y caminos en IPv6 no se encuentran saturados actualmente.

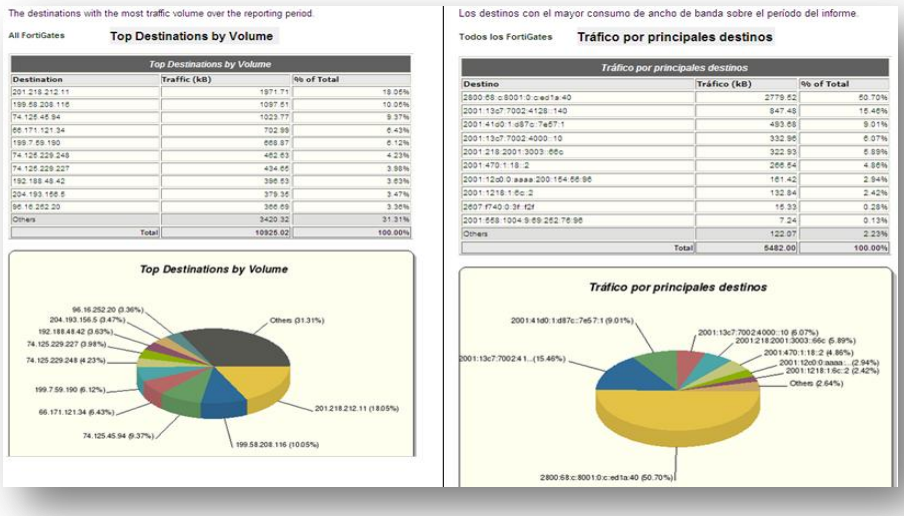

Figura 4-68. Principales destinos
Fuente: http://uio.ute.edu.ec/profesor/fvelaste/manuales
Elaborado por: El Autor

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

La implementación de IPv6 en la UTE permitirá darse cuenta de los nuevos beneficios que esta tecnología brinda, mencionando como uno de los principales la seguridad y disponibilidad.

En ciertos dispositivos de red en los que no se pueda implementar IPv6 por alguna razón, se manejará una solución de túnel en la que se coexistirá con IPv4.

Hoy en día prácticamente todos los sistemas operativos soportan IPv6 y los servicios que actualmente tiene la UTE en lo que se refiere servidores WEB y de Correo, están implementados con el software y hardware de última tecnología que garantizan una compatibilidad total con IPv6.

Muchos equipos de telecomunicaciones (*Routers*, S*witches* nivel3, Servidores de acceso, DSLAM, etc.) no vienen con IPv6 por omisión en todas las versiones, y esto tiene que ser un requisito en el momento de la inversión.

Una de las plataformas más empleadas en enrutamiento es la de Cisco, pero en la versiónIPv4, que es la que por omisión viene con muchos *Routers* sencillos y medianos, (IPv6 no estaba incluido aún se mantiene la situación, aunque habría que revisar la documentación actual de Cisco IOS); cualquier equipo de las series

3700/3800, viene sin soporte IPv6, excepto que se haya especificado en la compra y el vendedor haya actualizado el IOS o lo haya incluido en la cotización.

Los Puntos de Acceso inalámbricos AP que se tiene implementado en la Universidad no se los podrá administrar por IPv6, ya que su sistema operativo no es compatible, pero como se mencionó en el Capítulo IV, estos dispositivos permiten el paso del tráfico versión 6.

RECOMENDACIONES

Se recomienda tomar en cuenta todos los dispositivos y servicios que intervienen o forman parte de la red para que el momento de la implementación no se tome por sorpresa y represente un problema o pérdida de tiempo en la implementación

Se recomienda una verificación de pruebas que determinaran que la implementación y el proyecto se han realizado de acuerdo a los objetivos planteados.

En el momento de hacer el diseño de la red y la selección y cotización del equipamiento, es importante poner IPv6 como requisito, porque de esa manera el presupuesto ya incluye las actualizaciones en los equipos (que evidentemente aumenta un poco el presupuesto); pero cuando se está haciendo la inversión, en muchos casos es posible reajustar los presupuestos, y si la inversión es considerable, puede obtenerse soporte IPv6 sin incremento alguno en los costos iniciales. Una vez que ya se ha hecho la inversión, es complicado conseguir el dinero adicional que falta para hacer la actualización de los equipos. Por supuesto, mientras más grande sea la inversión a realizar, las cifras por concepto de actualización de sistemas operativos en los equipos de telecomunicaciones puede ser significativo.

Pese a que IPv6 provee una funcionalidad similar a la de IPv4, muchos de los mecanismos utilizados son diferentes. Por tal motivo requiere de un análisis cuidadoso. Las implicaciones de seguridad de IPv6 deben ser consideradas previas a su despliegue, para evitar un impacto negativo en las redes.

Dado que la mayoría de los sistemas de uso general cuenta con soporte IPv6, incluso los administradores de las redes IPv4 debería conocer las implicaciones de seguridad IPv6. Incluso si todavía no se ha planificado, es probable que se necesite desplegar IPv6 en el corto plazo. Por lo tanto hay que capacitarse y comenzar a implementar con IPv6

BIBLIOGRAFÍA

LIBROS

- BLACK, U. (2010). Redes (Primera ed.). España: Anaya Multimedia.

- PRESSMAN, R. S. (2002). Ingeniería de Software (Sexta ed.). Madrid: McGraw Hill D.L

- STALLINGS, W. (2003). Comunicaciones y Redes de Computadores (Sexta ed.). Mexico: Prentice Hall.

- STEWART, K., & Adams, A. (2003). Diseño y Soporte de Redes de Computadoras (Primera ed.). Mexico: Prentice Hall.

- TANENBAUM, A. (2003). Redes de Computadores (Sexta ed.). Mexico: Prentice Hall.

FUENTES ELECTRÓNICAS

TEMA CONSULTADO: Internet

- Sterling, B. (1992). Historia del internet. Obtenido el 15 de diciembre 2010, de http://biblioweb.sindominio.net/telematica/hist_internet.html

TEMA CONSULTADO: Modelo OSI

- Modelo Osi, [n.d]. Obtenido el 15 de diciembre 2010, de http://es.wikipedia.org/wiki/Modelo_OSI

- Arquitectura de Redes, [n.d]. Obtenido el 16 de diciembre 2010, de http://html.rincondelvago.com/arquitectura-de-redes.html

- Modelo Osi, [n.d]. Obtenido el 16 de diciembre 2010, de http://www.monografias.com/trabajos13/modosi/modosi.shtml

- Modelos de referencia de redes, (1996). Obtenido el 16 de diciembre 2010, de http://www.cs.virginia.edu/~knabe/iic3512/apuntes_3.html

TEMA CONSULTADO: IPv6

- IPv6, [n.d]. Obtenido el 18 de diciembre 2010, de http://es.wikipedia.org/wiki/IPv6

- Hernández, J. [2004]. Modelo Osi. Obtenido el 18 de diciembre 2010, de http://www.monografias.com/trabajos29/modelo-osi/modelo-osi.shtml

- Martínez, J. [2004]. El protocolo IPv6.Obtenido el 21 de diciembre 2010, de http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

- Rinkunosekai, [2008]. Redes Lan. Obtenido el 22 de diciembre 2010, de http://rinkunosekai.blogspot.es/1200676440/

TEMA CONSULTADO: TCP/IP

- El modelo TCP/IP, [n.d]. Obtenido el 13 de enero 2011, de http://technet.microsoft.com/es-es/library/cc786900(WS.10).aspx

- TCP/IP, [n.d]. Obtenido el 13 enero de 2011, de http://es.kioskea.net/contents/internet/tcpip.php3

- Chávez, J. [n.d]. Protocolo TCP/IP. Obtenido el 14 de enero 2011, de http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

- Soto, M. [n.d]. Protocolo TCP/IP. Obtenido el 18 de enero 2011, de http://usuarios.lycos.es/janjo/janjo1.html

- Modelo OSI y Capas TCP, [n.d]. Obtenido el 18 enero 2011, de http://preguntaslinux.org/-guia-modelo-osi-y-capas-tcp-t-19.html

TEMA CONSULTADO: RARP

- Protocolo resolución de direcciones inverso, [n.d].Obtenido el 25 de enero 2011, de http://es.wikipedia.org/wiki/Reverse_Address_Resolution_Protocol

TEMA CONSULTADO: Organismos de asignación direcciones IP

- Políticas IPv4, [n.d]. Obtenido el 27 de enero 2011, de http://www.nic.mx/es/IP.Politicas_IPv4

- Alojamiento web, [n.d]. Obtenido el 03 de febrero 2011, de http://es.wikipedia.org/wiki/Alojamiento_web

TEMA CONSULTADO: Paquetes y sockets

- Modelo OSI y Capas TCP, [n.d]. Obtenido el 18 enero 2011, de http://preguntaslinux.org/-guia-modelo-osi-y-capas-tcp-t-19.html

TEMA CONSULTADO: Formato de segmento TCP/IP

- Protocolo TCP/IP, [n.d]. Obtenido el 03 de febrero 2011, de http://es.kioskea.net/contents/internet/tcp.php3

- Rubio, J. (2005). TCP/IP Amenazas. Obtenido el 16 de febrero 2011, de http://profesores.is.escuelaing.edu.co/asignaturas/sypi20071/FOLLETOS%20Y%20MATERIAL%20DE%20ESTUDIO/TCPIP_Amenazas%20y%20protecci%F3n.pdf

TEMA CONSULTADO: UDP

- El protocol UDP, [n.d]. Obtenida el 16 de febrero 2011, de http://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/udp.html

ANEXOS

COMANDOS IPV6

Abrir una ventana de comandos (Inicio->Ejecutar->cmd) y escribir lo siguiente:

netsh interface IPv6 add address interface_nameIPv6_address

Por ejemplo, para configurar una dirección IPv6unicast 2001:db8:290c:1291::1 en la interfaz “Conexión de Área Local” con un valor infinito para los parámetros “validlifetime” y “preferredlifetime” y hacer que este cambio sea persistente (no cambie cada vez que se reinicia el sistema):

netsh interface IPv6 add address "Conexión de Area Local"

2001:db8:290c:1291::1

Configuración de la selección de la dirección

“En IPv6, cada interfaz físico de red puede tener múltiples direcciones asignadas a los interfaces lógicos de red o a túneles por varios motivos. Por esta razón, el RFC3484 proporciona un método estandarizado para elegir la dirección IPv6 fuente y destino con la que se va a intentar realizar una conexión.

Este RFC define dos algoritmos:

1. Un algoritmo para la selección de la dirección de destino para formar una lista de posibles direcciones destino ordenada por preferencia.
2. Un algoritmo de selección de direcciones fuente para elegir la dirección que mejor se adapta a la dirección de destino.

Estos algoritmos se implementan en el Sistema Operativo para que las aplicaciones no tengan que incluir su propio algoritmo de selección. Sin embargo, las aplicaciones pueden puentear el algoritmo si usan direcciones físicas en vez de usar nombres de dominio para contactar con servidores remotos.

En Windows XP, 2003 y Vista para tener control administrativo sobre la precedencia de las direcciones fuente/destino existe una tabla local de políticas de prefijos que se puede configurar como se muestra a continuación:

netsh interface IPv6 show prefixpolicy --> muestra la tabla local de políticas de prefijos.

netsh interface IPv6addprefixpolicy --> añade nuevas entradas a la tabla local de políticas de prefijos.

netsh interface IPv6 set prefixpolicy --> configura entradas en la tabla local de políticas de prefijos .

netsh interface IPv6deleteprefixpolicy --> borra entradas en la tabla local de políticas de prefijos.

Ejemplo:

C:\>netsh interface IPv6 show prefixpolicy

Precedence	Label	Prefix
5	5	2001::/32
10	4	::ffff:0:0/96
20	3	::/96
30	2	2002::/16
40	1	::/0
50	0	::1/128

La tabla anterior muestra lo siguiente:

1) Si está disponible la conectividad IPv6 nativa, cualquier destino IPv6 tiene mayor precedencia que cualquier destino IPv4:

10 4 ::ffff:0:0/96 ==>cualquierdirecciónIPv4
40 1 ::/0 ==>cualquierdirecciónIPv6

2) Si está disponible el mecanismo de transición 6to4 en el PC, cualquier destino IPv6 tiene mayor precedencia que cualquier destino IPv4:

10 4 ::ffff:0:0/96 ==>cualquierdirecciónIPv4
40 1 ::/0 ==>cualquierdirecciónIPv6 6to4

3) Si está disponible el mecanismo de transición Teredo en el PC, cualquier destino IPv4 tiene mayor precedencia que cualquier destino IPv6:

10 5 2001::/32 ==>cualquierdirecciónIPv6Teredo
40 1 ::ffff:0:0/96 ==>cualquierdirecciónIPv4

Cambiar la precedencia en la selección de direcciones.

Si quieres cambiar la precedencia de un prefijo, por ejemplo el de Teredo para tener mayor precedencia que la direcciones IPv4, entonces según la tabla de políticas de prefijos anterior, lo que habría que hacer es:

C:\>netsh interface IPv6 set prefixpolicy prefix=2001::/32 precedence=15 label=5

Deshabilitar IPv6

A diferencia de lo que ocurre en Windows XP y 2003, IPv6 en Windows Vista no se puede desinstalar porque es parte integrante de la pila IP. Para deshabilitar IPv6 en una conexión o interfaz de red específicos hay que ir a la carpeta “Conexiones de Red”, obtener las propiedades de la conexión o interfaz de red y deseleccionar el componente “Protocolo Internet versión 6 (TCP/IPv6)” de la lista. Este método deshabilita IPv6 de dicha conexión o interfaz de red pero no deshabilita IPv6 de los interfaces de túneles ni de la interfaz virtual loopback.

Para deshabilitar de manera selectiva algunos componentes de IPv6 o configurar su comportamiento, en Windows Vista hay que crear y configura el siguiente valor del registro de Windows (tipo DWORD)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters\DisabledComponents.

Disabled Components está configurado a 0 por defecto.

El valor de registro Disabled Components es una máscara de bits que controla los siguientes parámetros, comenzando por el bit de menor orden (Bit 0):

Bit 0 puesto a 1 para deshabilitar todos los interfaces de túnel IPv6, incluyendo ISATAP, 6to4, and Teredo. El valor por defecto es 0.
Bit 1 puesto a 1 para deshabilitar todos los interfaces de túnel 6to4. El valor por defecto es 0.
Bit 2 puesto a 1 para deshabilitar todos los interfaces ISATAP. El valor por defecto es 0.
Bit 3 puesto a 1 para deshabilitar todos los interfaces Teredo. El valor por defecto es 0.
Bit 4 puesto a 1 para deshabilitar IPv6 sobre todos los interfaces que no son túneles, incluyendo interfaces LAN y PPP. El valor por defecto es 0.
Bit 5 puesto a 1 para modificar la tabla de políticas de prefijos y preferir IPv4 sobre IPv6 en las conexiones. El valor por defecto es 0.

Para determinar el valor del parámetro *Disabled Components* para una determinada configuración hay que construir un número binario con el valor adecuado y después convertirlo a su valor hexadecimal. Por ejemplo, si quieres deshabilitar los interfaces 6to4 y Teredo y preferir IPv4 sobre IPv6entonces habría que construir el siguiente número binario: 101010. Después convertirlo a su valor hexadecimal de manera que el valor del parámetro DisableComponents sería 0x2A.

La siguiente tabla muestra algunas combinaciones de configuraciones típicas correspondientes al valor del parámetro DisabledComponents.

Configuración	valor DisabledComponents
Deshabilitartodos los túneles	0x1
Deshabilitar 6to4	0x2
Deshabilitar ISATAP	0x4
DeshabilitarTeredo	0x8
DeshabilitarTeredo y 6to4	0xA
Deshabilitar todos los interfaces LAN y PPP	0x10
Deshabilitar todos los interfaces LAN, PPP y túneles	0x11
PreferirIPv4 a IPv6	0x20
Deshabilitar IPv6 en todos los interfaces y preferir IPv4 a IPv6	0xFF

Después de hacer estos cambios hay que reiniciar el PC para que el nuevo valor de DisableComponents tenga efecto. “